**Journal of Artificial Intelligence, Machine Learning and Neural Network**
**ISSN:2799-1172**
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
**DOI:** https://doi.org/10.55529/jaimlnn.26.32.42

# Implementation of Artificial Intelligence in a Software-Defined Wireless Sensor Network

**Dr. Santosh Kumar[1], Piyush Raja[2*]**

*[1,2*]Assistant Professor, Department of CSE, COER University, Roorkee, Uttarakhand, India*

*Corresponding Email: [2*]piyushraja2009@gmail.com*

**Received:** 09 August 2022 **Accepted:** 25 October 2022 **Published:** 27 November 2022

***Abstract:*** ***Incorporating a Software-Defined Network (SDN) paradigm into a Wireless Sensors Network makes it possible to realise Software-Defined Wireless Sensor Networks (SDWSNs), also known as Software-Defined Wireless Sensor Networks (WSN). The reason for this is to investigate and discover answers to the issues that are brought about by WSN. Both artificial intelligence (AI) and machine learning play a key role in our culture and are assisting in the development of systems that are able to manage themselves on their own. Our culture is influenced significantly by both of these. WSNs have found use in a wide variety of industrial applications, including some in which the network's performance and dependability are of the utmost importance to the accomplishment of the overall project. Using a wide array of cutting-edge AI approaches can considerably improve both the usability and dependability of these apps. This can be accomplished by enhancing the functionality of the implementations. Looking further into application of Artificial Intelligence SDN techniques might result in advances in network management, security, or routing in SDWSN. If these issues are addressed, the network may become more reliable. In this paper, we examine the application of machine learning algorithms in software-defined networks (SDN) and analyse the prospect of utilising these AI in software-defined wireless sensor networks (SDWSN) to overcome the challenges presented by WSN and increase the performance as well as the dependability of the system.***

***Keywords: WSN, SDWSN, Machine Learning, Security, Routing.***

## 1. INTRODUCTION

WSNs may be used to create robust apps with application requiring its own unique set of criteria and including its unique set of characteristics. WSN is accompanied by a number of design criteria, some examples of which are localization, energy-conscious routes, accuracy, network grouping, and notification, fault detection, and so on. Radio communication, which encompasses both the sending and receiving of data, is the activity that makes the most

**Journal of Artificial Intelligence, Machine Learning and Neural Network**
**ISSN:2799-1172**
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
**DOI:** https://doi.org/10.55529/jaimlnn.26.32.42

substantial contribution to the overall energy load of WSN. When it comes to WSN, routing is an extra area of interest; the following are the three primary motivating factors for the development of efficient routing systems:

1) The necessity of a guarantee for quality assurance of services (QoS)
2) Businesses in the telecommunications industry that have recently been deregulated; and
3) Rapid expansion in both the size of networks and the number of people using them [19].

WSN security is an additional concern, and attacks on WSNs can be divided into the following three categories: 1) An emphasis on the final product, which includes both passive and active attacks; 2) An emphasis on the performer, which encompasses both external and internal attacks; and 3) A focus on layers (connection requests architecture elements, such as the OSI model or User equipment) [20].

A number of different academics have come to the conclusion that a Software Defined Network (SDN) could be a viable solution to the problems that are caused by WSN. This is due to the difficulties that are encountered by WSNs as well as the growing demand for devices that are relevant to WSNs and Internet of Thing (IoT) gadgets that are making their way onto the market. Both of these factors contributed to this result. The software-defined network, or SDN, is a framework that is defined as a method that makes it possible for network managers to monitor and operate a large number of network devices in a manner that is both autonomous and dynamic. In addition, software-defined networking (SDN) makes it possible to physically divide the network's control plane and forwarding plane from one another [23].

SDN is required for a number of reasons, including virtualization (the use of network resources without regard to their physical location), orchestration, programmability (the ability robotics, effectiveness (improving base station and potential, packet forwarding, the throughput administration), dynamical expansion (as capability to modify quantities or breadth), etc partnership working. Virtualization is the use of network resources without regard to their physical location. Programmability is the ability to change. The implementation of SDN into WSN resulted in the formation of the acronym SDWSN (software defined wireless sensor network). The article [21] discusses the significance of software-defined networking in wireless sensor networks. The writers propose a solution to the difficulties that arise in WSN that is based on SDN, and the authors examine the significance of SDN in wireless sensor networks. The authors state that the controller, which is equipped with an acceptable quantity of power resources, will be the location where the functions that demand a significant amount of power will be kept. SDN provides an additional answer to the issues that arise in this environment by making it possible for the controller to handle the routing, mobility, and localization responsibilities in WSN. In addition, the utilisation of SDN can lead to an enhanced management of large-scale WSN [21], which is something that can be performed.

**Journal of Artificial Intelligence, Machine Learning and Neural Network**
**ISSN:2799-1172**
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
**DOI:** https://doi.org/10.55529/jaimlnn.26.32.42

Regardless of these answers, academics are often searching for some further approaches to address problems and develop methods for improving energy and power consumption, developing effective methods for routing in networks, and developing methods for protecting this network. Even with these answers, academics are always seeking for new approaches to handle problems and find solutions. Even with these answers, academics are always seeking for new approaches to handle problems and find solutions. The use of SDN in WSN does address a significant number that are encountered in WSNs; however, this does not mean that all of the challenges have been resolved. Researchers have recently been mulling over the possibility of implementing AI in SDWSN in order to cut down on energy usage, improve network routing, and bolster network security. The process of machine learning is one that is utilised by a sizeable portion of the scientific community's researchers today. The importance of artificial intelligence and machine learning in wireless sensor networks may primarily be broken down into the following categories:

• Because data is occasionally collected in areas that are occasionally inaccessible, dangerous, or unpredictable, having a self-calibration network will be absolutely necessary.
• Because sensor nodes are used to monitor the changes that occur in dynamic settings over time, which themselves are subject to change, sensor nodes themselves have to be able to adapt and function well.

The author of "25" investigates numerous applications of artificial intelligence (AI) to different areas of software-defined networking (SDN), most notably routing, network management, and network security. The primary focus of Bai's [26] study was on the difficulties associated with network routing that can be alleviated by the utilisation of AI. Despite this, the potential for utilising AI strategies in SDWSN will be the primary focus of the attention paid to this topic throughout this work. As a consequence of this, we will highlight some of the existing gaps in knowledge while examining and analysing some of the work that has been completed. This will be done while simultaneously reviewing and analysing some of the work that has been done. In conclusion, Lets list various programs in brief. that have been discussed, with an emphasis on the applications of these algorithms, the AI technique that has been used, the aims, and the barriers that still need to be overcome.

The Function of AI in the Organization and Management of Transportation Routing It would appear that scientists and engineers are finding Artificial Intelligence to be an appealing problem in virtually every scientific field that they research. It was a subject that was brought up in conversations about cognitive capability of technology. Those domains in which investigators having applied Machine learning or approaches as a strategy for SDN would be covered in the following section. the intention of also employing them in SDWSN. This section will focus on applications that have the potential to be used in SDWSN.

**Pathfinding**
A network has the flexibility to deliver data to a specific location when it is able to route data packets to multiple nodes within the network. This allows the data to be delivered directly to the point at which it is required. Overload scenarios, severely loaded networks, minimally

**Journal of Artificial Intelligence, Machine Learning and Neural Network**
**ISSN:2799-1172**
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
**DOI:** https://doi.org/10.55529/jaimlnn.26.32.42

loaded networks, and variable traffic patterns are all things that the network should be able to sustain [19]. It is the responsibility of the network's routing mechanism to ensure that data may move freely throughout the network between any two end points, and the network itself should be able to accommodate networks that are either significantly or lightly loaded. The research that is presented in [25] provides an introduction to the fundamentals of the load balancing function, which is a requirement for maximising the throughput of a computer network and minimising its latency to the greatest extent possible in order to support a variety of routing strategies.

When it comes to software-defined networking (SDN), there have only been a select few AI-based algorithms developed so far in order to address routing and quality of service (QoS) traffic classification [25]. The latency of the back propagation neural network, commonly known as BPNN, has been lowered by 19.3 percent when compared to alternative methods, such as static round robin methods. Utilizing this strategy allows for real-time dynamic load balancing to be achieved. There is a significant reduction in the amount of time spent transmitting routing decisions from the controller to the Open vSwitch [27] thanks to the utilisation of the BPNN. This is accomplished by having it applied locally within the Open switch application itself. Ant Colony Optimization (ACO) is another algorithm that is based on how ants behave in order to identify the optimum method to travel from their food supply to their nest. This algorithm was named after the ants that were used as the inspiration for the algorithm. Google is responsible for the development of this algorithm, which is known as Ant Colony Optimization (ACO). The SDN application in the SDN controller runs ACO algorithms on a weighted graph; the weights are calculated to reflect the loss rate and latency that are experienced in each network device. The Quality of Experience (QoE) value that was achieved by ACO has enhanced by 24.1% in contrast to that which was attained by the shortest path approach [28].

The majority of the work that has been done with AI to tackle routing problems can be categorised as falling under the following category of algorithms: algorithmic resource allocation methods, shortest path algorithms, and distributed AI and agent based routing. This is because AI can be used to tackle routing problems in a decentralised manner.

There has been an increase in the amount of research carried out to enhance the Quality of Service (QoS) of routers. A framework for QoS-aware traffic classification using semi-supervised machine learning was suggested by the authors of [30]. [Citation needed] When software-defined networking (SDN) is used to manage network traffic based on flows, the accuracy and efficiency of the traffic classification (TC) engine plays a significant role in SDN. As a direct consequence of this, we are going to have to reconsider and rethink the SDN traffic engineering solutions. Because of this, we will be able to make use of the capabilities offered by SDN. The task of ascribing a Quality of Service (QoS) class to a flow of traffic in order to enable the selection of an appropriate routing path is the job of the TC engine. When new devices are introduced, this becomes a problem, and it can sometimes become difficult to identify the QoS class of the traffic flows.

**Journal of Artificial Intelligence, Machine Learning and Neural Network**
**ISSN:2799-1172**
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
**DOI:** https://doi.org/10.55529/jaimlnn.26.32.42

**Direction and Control of the Flow of Traffic**

An efficient technique that is capable of detecting QoS classes, choosing an acceptable path even when new applications are launched, and reducing the need to continually maintain a real-time update of the whole list of programmes that are accessible through the internet is described here. The structure that is being proposed is comprised of the two components that are as follows: 1) the component for local traffic identification that is placed in SD-switches at the edge of the network, and 2) the global traffic classifier that is situated in the network controller. Both of these components can be found in the network controller. The following three advantages are provided by this proposed classification system: I the SD-switches are kept as simple as possible by only incorporating lightweight elephant flow identification; ii) the network controller is utilised to guarantee the accuracy and the adaptability of the QoS classifier; and iii) the entire framework adheres to a modular design principle so that every component in the framework can be improved at any time; iv) the modular design principle ensures that the framework can be improved at any time. This method that has been described for classifying QoS is one that can be applied in SDN to enable fine-grained QoS-aware traffic engineering.

The framework that is proposed in [29] makes an effort to classify a traffic flow into a Quality of Service category in real time and in an adaptable manner. This is done without the need to identify the particular application that is responsible for generating the traffic flow. A QoS scoring algorithm is utilised in order to achieve this goal successfully. You'll be able to locate the TC engine within the centralised SDN controller. The TC engine is responsible for the following functions: a) efficient network monitoring with very little overhead and very few switch adjustments; b) the identification of QoS critical flows; c) the QoS-aware classification of traffic; and d) the enabling of services such as application discovery by making use of Deep Packet Inspection while it is running in the network controller.

Since the data found in the stream is not always adequately labelled, the algorithms have trouble dealing with the unlabelled data. Despite the fact that the purpose of semi-supervised machine learning (also known as semi-ML), which stands for semi-supervised machine learning, is to mix the concepts of supervised machine learning algorithms and unsupervised machine learning algorithms, the term semi-ML still applies. It is essential to perform deeper research into this subject using the principles of supervised and unsupervised machine learning algorithms to apply to SDWSN. In addition, when they were conducting an analysis of the algorithm that they had investigated, they were unable to find an accurate way for checking the accuracy of their conclusions. This was a problem for them because they had already spent time researching the algorithm. This occurred because unlabeled flows, after being processed by the classifier, were unable to be checked with an unknown application. The reason for this was owing to the fact that unlabeled flows. As a consequence of this, extra research is required in order to evaluate the precision of the unlabeled data that was acquired from the examination of the data that was submitted.

**AI in Security**

Because a hacked network might give unauthorised access to crucial information, could be used to launch attacks on other users, or could even bring the internet to a halt, it is always

**Journal of Artificial Intelligence, Machine Learning and Neural Network**
**ISSN:2799-1172**
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
**DOI:** https://doi.org/10.55529/jaimlnn.26.32.42

necessary to maintain a connection to a secure network. The ever-increasing sophistication of technology makes it necessary to develop networks that are both swift and dependable; in addition, the level of security must be raised, particularly in view of the expanding number of possible risks that could be posed. The security measures that are put in place in networks need to be able to adapt to new dangers, which includes both learning from previous dangers that have been identified and adapting to the development of new techniques to combat new dangers. In other words, adaptability is essential for network security. It is conceivable to provide network security the ability to adapt and react to new threats as they emerge using AI and machine learning techniques. This would make network security more proactive. Machine learning is currently the most successful technique for dealing with this difficulty. This is due to the fact that every threat, regardless of how innovative it may be, follows a pattern.

**i) By Using Some Kind of Formula or Algorithm It's officially known as the Support Vector Machine.**

Wang et al. [31] utilised support vector machine in the process of developing an algorithm for the aim of monitoring security in SDN (SVM). SVM stands for support vector machine and is a technique for supervised learning that is utilised to analyse data and recognise patterns; the major application of this approach is to cluster data. The proposed method lays the primary emphasis not only on the classification of hazards in network intrusion detection system (NIDS), but also on the control of network traffic (NIDS). The development of an algorithm that is capable of monitoring data flow within the network and providing security against dangers posed by SDN is the objective of this technique. This is the impetus behind utilising this strategy.

**ii). Putting an Algorithm for Machine Learning Into Practice Using a System of Partial Supervision**

In this post, we take a look at four distinct machine learning algorithms and discuss how they stack up against one another. This machine learning algorithm's objective is to bolster the IDS's defences against DDoS assaults, and its primary tool will be reinforcement learning. The assaults begin by being launched at the network layer; if this attempt is unsuccessful, the attacks then shift to the application layer and overwhelm it with HTTP GET messages [20], [32]. [Note: The IDS-based approach that has been proposed incorporates the two modules listed below: I the first module is a sophisticated signature-based intrusion detection system (IDS) that analyses requests and determines whether or not the hosts have normal or abnormal behaviour; ii the second module examines packets that are transmitted from hosts in order to determine whether or not they are suspicious. The first module is constructed using strategies that are taken from machine learning.

The "anomalous behaviour detection" method utilises machine learning techniques one more time before beginning to transmit a packet in order to identify whether or not the packet contains data that could be considered malicious. If it is determined that the packet was part of a DDoS attack, the system will update the flow table and identify the host from which the infected packet was sent. We need to discover a way to improve the algorithm because there

**Journal of Artificial Intelligence, Machine Learning and Neural Network**
**ISSN:2799-1172**
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
**DOI:** https://doi.org/10.55529/jaimlnn.26.32.42

is no guarantee that the host will continue to provide infected packets on a constant basis. This makes it necessary for us to find a solution. This method is sufficient for preventing DDoS attacks; however, the problem with it is that the host that sent the packet with the DDoS will become unusable the next time because its address will be added to the list of blocked hosts. Although this method is sufficient for preventing DDoS attacks, the problem with it is that it makes the host that sent the packet with the DDoS unusable.

**AI In Admission Control**

One of the many activities that are done by the SDN controller when it receives a request for connection is the admission control, which is also one of the tasks that is considered to be one of the most significant jobs (AC). The AC controller is responsible for handling the service request if there is a significant amount of demand placed on the network. If resources are available AC acknowledges request and if not dismisses the request. The AC strategies that are now being utilised are threshold-based; more specifically, they make use of minimum, maximum, exclusive, and non-exclusive constraints on resource sections that the network operator can impose for a variety of different categories of flows.

**AI IN SDWSN**

**i). A protocol for making effective use of power in the routing of computer networks utilizing the Techniques of the Reinforcement Learning Process**

The majority of work that is done on SDWSN using AI focuses on monitoring energy efficiency for routing. This is because it is one of the most important aspects of the network. A new energy-efficient routing algorithm for SDWSN has been created. In this algorithm, control nodes are entrusted with carrying out a number of different dynamic operations. They used a non-linear weight particle swarm optimization algorithm to create a cluster structure so as to minimise the transmission distance in order to optimise the energy consumption of the network [23]. This allowed them to create a cluster structure that used the least amount of energy possible. Because of this, they were able to build a cluster structure that reduced the amount of energy that was needed for the network to transport data to its users. In this research, we suggest a monitoring strategy for SDWSN that makes use of the RL algorithm and is more efficient in terms of energy consumption. In order to improve the energy efficiency and self-adaptability of WSNs to variations in the surrounding environment, the RL algorithm was designed in such a way that it would execute value-redundancy filtering and load-balancing routing according to the values and distribution of flows, respectively. This was done in order to maximise the potential of WSNs to communicate with one another.
The proposed algorithm provides energy-efficient routing by monitoring data flows and taking account of each flow. As a consequence, the network is in a better position to effectively handle request connections. In the event that another packet is delivered with the same address as a previously transmitted packet, the nodes are able to simply forward the node since they have been able to keep track of each flow in the network. They are spared the hassle of having to recalculate the route as a result of this.

**Journal of Artificial Intelligence, Machine Learning and Neural Network**
**ISSN:2799-1172**
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
**DOI:** https://doi.org/10.55529/jaimlnn.26.32.42

**ii). Monitoring that is effective in terms of making efficient use of energy through reinforcement learning**

The information processing method that is based on RL is incorporated into the control plane of the network. Within this control plane, the interaction between agents and their environments is used to strengthen the intelligence in policy making in order to improve the self-adaptability of the energy-saving mechanism [30]. This is done in order to reduce the amount of energy that is wasted. This strategy ensures a higher quality of service by mining the application-specific value distribution and reducing the redundancy of data flows (QoS). This is intended to take into account the limitations that are imposed by WSNs, which can be described in terms of radio sources, energy, and computational capabilities.

According to the results of the experiments, the prototype of the system has the potential to improve energy efficiency through the effective inhibition of the transmission of value-redundant loads, the reduction in the amount of cross-plane communications, and the enhancement of the load balance in SDWSN. These improvements were made possible as a result of the system's ability to improve load balance. The proposed system does provide a good energy mechanism; nevertheless, it is not scalable in the sense that the control plane is concerned.

**iii). The Assurance and Safety of SDWSN**

Intruders are continuously looking for new entry points into networks, which is one of the main reasons why network security is such a crucial concern. Intruders can come from the inside (by attempting to enhance their access privileges in order to misuse non-authorized privileges) or from the outside. Intruders from the inside can exploit non-authorized privileges (targets network trying to gain unauthorised access to system information). There are many different kinds of intrusion detection systems (IDS), including active and passive intrusion detection systems (IDS), network intrusion detection systems (NIDS) and host intrusion detection systems (HIDS), knowledge-based and behavior-based (anomaly-based) intrusion detection systems (IDS), and so on and so forth. When used in the conventional fashion, this IDS has a drawback: passive IDS are incapable of performing any protective or corrective activities on their own. This limits their usefulness.

It is difficult for HIDS to conduct examinations of attempts at infiltration on multiple machines at the same time. Keeping huge networks with a wide variety of operating systems and configurations operational is another one of HIDS's many challenges. Knowledge-based intrusion detection systems need to be constantly updated and maintained; but, because of this requirement, they are unable to identify newly emerging threats. The behavior-based IDS is responsible for a significant number of false positive warnings. Because of these drawbacks, we are making an effort to create machine learning algorithms that seek to tackle this issue; the launch of intelligent IDS will be the consequence of this.

**Journal of Artificial Intelligence, Machine Learning and Neural Network**
**ISSN:2799-1172**
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
**DOI:** https://doi.org/10.55529/jaimlnn.26.32.42

## 2. SUMMARY AND DISCUSSION

A framework that provides Quality of Service (QoS) traffic classification in routers was established by both the QAR study and the other research. See the following table (I) for further details. The use of machine learning approaches in this research has the goals of monitoring traffic in the network and improving the routing capabilities of the network. Both of these goals can reduce the amount of delay time and flooding of packets that occur in the network, so the use of these approaches is important. Both of these procedures include the sending of packets to a variety of nodes or stations, therefore this is a factor that is common to both of them. It is essential that packets be routed efficiently and that the routing process be monitored to ensure that routers are not overburdened with packets coming from a range of nodes. It is also essential that effective packet routing be performed.

Examples of these tasks include choosing the correct path, monitoring the path for corrupt data, and being able to handle an increase in the flow of data traffic. Other possible obstacles include the following:

Summary Table

| Reference | Application | AI technique | Objective | Challenges |
|---|---|---|---|---|
| Chen-xiao et al. | Routing | Network with back propagation of brain activity | real time dynamic load balance to decrease the latency | Efficient use of energy |
| Dobrijevic et al. | Routing | Ant Optimization of the Colony's | Improve QoE | Managing traffic There are challenges involved in managing real-time traffic flow. |
| Kaur et al. | Routing | QAR by the Use of Reinforcement Learning | Improve QoS | It is difficult to keep track of all the data, particularly with new gadgets joining all the time. |
| Wang et al. | Traffic classification | Laplacian SVM | Classifies data flows to efficiently save energy | Difficult to keep track of all data especially with new devices connecting |
| Xiang et al. | Routing | Particle optimization swarm | Energy Beffcient routing | Demands a large number of control nodes in order to consume less energy; |
| Wang el al. | Security | Improved based SVM behaviour | DDos detection | Difficulty in adjusting to new data |
| Barki el al. | Security | 1.Naïve bayes 2.K nearest neighbor 3.K means, 4.K | DDoS and DoS attack detection | Difficulty in adjusting to new data |

**Journal of Artificial Intelligence, Machine Learning and Neural Network**
**ISSN:2799-1172**
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
**DOI:** https://doi.org/10.55529/jaimlnn.26.32.42

| | | | | |
|---|---|---|---|---|
| | | medoids | | |
| Leguay et al. | Admission Control | Cost-Sensitive | Connection request validation | Every day, a large number of connection requests are received, and unfortunately, some of them can't be approved. |
| Huang et al. | Energy-Effciency monitoring | Reinforcement Learning | To monitor energy efficiency | Scalability of the network is difficult to maintain successfully |

## 3. CONCLUSION

In this study, we examine earlier AI-related work with the intention of improving SDN's routing and security capabilities. When applied to networks, AI makes them more intelligent, reliable, and secure; it can also speed up the time it takes to detect and stop attacks on the network and reduce the amount of traffic that is lost during a flood. Artificial intelligence in SDWSN will usher in smart networks that can automatically adjust to changing conditions, calibrate themselves, and keep tabs on traffic. Also, these networks will be able to decide matters on their own, with no outside interference. With so many new applications being released every day, it is imperative that SDWSN employ the AI algorithms outlined in table I in order to function effectively. However, we do anticipate difficulties, and further study can be undertaken to determine what kind of improvement to the techniques discussed should be implemented to provide efficient routing, security, or energy-efficient monitoring to the network in order to meet necessary Quality of Service and Quality of Experience standards.

## 4. REFERENCES

1. F. Wortmann and K. Flüchter, ‘‘Internet of Things,’’ Bus. Inf. Syst. Eng., vol. 57, no. 3, pp. 221–224, 2015.
2. Fog Computing and the Internet of Things: Extend the Cloud to Where the Things are, Cisco Syst., San Jose, CA, USA, 2016.
3. Y. Jarraya, T. Madi, and M. Debbabi, ‘‘A survey and a layered taxonomy of software-defined networking,’’ IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 1955–1980, 4th Quart., 2014.
4. F. Hu, Q. Hao, and K. Bao, ‘‘A survey on software-defined network and OpenFlow: From concept to implementation,’’ IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 2181–2206, 4th Quart., 2014.
5. A. M. Abu-Mahfouz, T. Olwal, A. Kurien, J. L. Munda, and K. Djouani, “Toward developing a distributed autonomous energy management system (DAEMS),” in Proc. of the IEEE AFRICON 2015 Conference on Green Innovation for African Renaissancce, 2015, pp. 1–6.

**Journal of Artificial Intelligence, Machine Learning and Neural Network**
**ISSN:2799-1172**
Vol: 02, No. 06, Oct-Nov 2022
http://journal.hmjournals.com/index.php/JAIMLNN
**DOI:** https://doi.org/10.55529/jaimlnn.26.32.42

6. P. Dongbaare, S. P. Chowdhury, T. O. Olwal, and A. M. Abu-Mahfouz, "Smart Energy Management System based on an Automated Distributed Load Limiting Mechanism and Multi-Power Switching Technique," in Proceedings of the 51st International Universities' Power Engineering Conference, 2016.
7. M. J. Mudumbe and A. M. Abu-Mahfouz, "Smart water meter system for user-centric consumption measurement," in Proc. of the IEEE International Conference on Industrial Informatics, 2015, pp. 993–998.
8. A. M. Abu-Mahfouz, Y. Hamam, P. R. Page, and K. Djouani, "Real- time dynamic hydraulic model for potable water loss reduction," Procedia Eng., vol. 154, no. 7, pp. 99–106, 2016.
9. B. Cheng, L. Cui, W. Jia, W. Zhao, and P. H. Gerhard, "Multiple Region of Interest Coverage in Camera Sensor Networks for Tele-Intensive Care Units," IEEE Trans. Ind. Informatics, vol. 12, no. 6, pp. 2331–2341, Dec. 2016.
10. B. Silva, R. M. Fisher, A. Kumar, and G. P. Hancke, "Experimental Link Quality Characterization of Wireless Sensor Networks for Underground Monitoring," IEEE Trans. Ind. Informatics, vol. 11, no. 5, pp. 1099–1110, Oct. 2015.