International Journal of Computing and Artificial Intelligence

E-ISSN: 2707-658X
P-ISSN: 2707-6571
IJCAI 2021; 2(1): 62-68
Received: 22-11-2020
Accepted: 25-12-2020

Kadiri Kamoru Oluwatoyin
Department of Electrical and Electronic Engineering, Federal Polytechnic, Offa Kwara State, Nigeria

Abubakar Dauda
Department of Information and Communication Technology, National Control, Centre/Transmission Control Centre, Osogbo, Nigeria

Enem Theophilus Aniemeka
Department of Computer Science, Air Force Institute of Technology, Nigerian Air Force Base, Kaduna, Nigeria

Corresponding Author:
Kadiri Kamoru Oluwatoyin
Department of Electrical and Electronic Engineering, Federal Polytechnic, Offa Kwara State, Nigeria

Development of machine language for internet of things

Kadiri Kamoru Oluwatoyin, Abubakar Dauda and Enem Theophilus Aniemeka

DOI: https://doi.org/10.33545/27076571.2021.v2.i1a.28

Abstract
The fast growth in the number of smart devices capable of running complex apps significantly impacts the information communication technology industry's landscape. The Internet of Things (IoT) continues to grow in popularity and relevance in man's daily existence. However, as the Internet of Things evolves, so do the associated problems. Thus, the need for IoT development and ongoing upgrading becomes stronger. To maximize the potential of IoT systems, machine learning technologies have recently been used. The implementation of machine learning algorithms in IoT systems is examined in detail in this paper. Two categories of machine learning-based IoT algorithms deal with fundamental IoT challenges like localization, clustering, routing, and data aggregation. Additional machine learning-based IoT algorithms deal with performance challenges like congestion control, fault detection, resource management, and security.

Keywords: Wireless sensor networks (WSNs), machine learning, unsupervised learning, supervised learning, internet of things (IoT)

1. Introduction
The Internet of Things (IoT) refers to a networking architecture that permits ubiquitous computing is pervasive and distributed services. The Internet of Things (IoT) is a network of interconnected gadgets and items that connect to the Internet and their surroundings. Everyday goods, such as sensors and smartphones/devices, may be linked to form a vast, interconnected system called the Internet of Things. About 50 billion IoT devices will be in use globally by 2020, producing more than 60 ZB data (Van der 2017; Sam 2016) [34, 32]. The Internet of Things will be made up of wireless sensor networks (WSNs) (IoT). Many people have been interested in WSNs in the last several years. The definition of a WSN includes a set of application-specific sensor nodes equipped with communication modules.
Information gathered by the nodes is used to detect and record various environmental conditions. Notably, air temperature, humidity, wind speed, and wind direction are among the factors most often measured. The application-specific system development industry is highly suitable for WSNs. To work together and accomplish their jobs, sensor nodes in the IoT need a combination of WSNs and IoT. Both IoT and WSNs have a range of issues and concerns that must be solved. Energy efficiency, node placement, event schedule, route construction, data aggregation, defect detection, and data security are just a few applications for many systems. Due to the application of machine learning, this issue may be resolved. IoT performance and distribution will be significantly improved using machine learning. ML was first used as an approach to artificial intelligence in the 1960s (Ayodele 2010) [6]. Efforts to improve the resilience, effectiveness, and accuracy of algorithms have been continuous since that time. Machines that use machine learning algorithms to aid in a wide variety of applications, including bioinformatics, face and voice recognition, agricultural monitoring, fraud detection, and marketing, are often used today. Autonomous machine learning may be used to increase IoT systems' performance by analyzing previously gathered data and identifying the activities that led to better performance, and automating that process to perform better without the need to reprogram it. Machine learning plays a critical role in IoT applications because of the following:

- IoT devices' monitoring of dynamic surroundings. Because of this, IoT systems that respond automatically to changes must be implemented.
- Exploratory Internet of Things applications, like wastewater monitoring and volcanic

Eruption monitoring, use disreputable and unsafe sites to get new data. Consequently, machine learning-based IoT systems must be able to self-calibrate in response to new inputs to provide robustness.

- Machine learning improves not just autonomous control but also the capacity of IoT apps to make intelligent judgments. Nonetheless, some issues must be carefully considered when using machine learning in IoT.

IoT devices, for example, have resource limits. In IoT devices, using machine learning to identify consensus relationships between obtained data samples and to predict viable hypotheses uses a lot of energy. This necessitates a trade-off between the machine learning algorithm's computing cost and the required accuracy of the learning process.

The concept, history, architecture, and data processing levels of the Internet of Things are covered in this paper. Machine learning methods include supervised learning and unsupervised learning, plus reinforcement learning, evolutionary computation, and fuzzy logic. We investigate the applicability of machine learning algorithms to IoT challenges in depth. In addition, we separate applications like this into two types: those that operate the IoT system and those that improve the system's performance.

1.1 An introduction to IoT

IoT is a network of "things" (like smartphones, tablets, and smart TVs) that automatically detect, collect, and send data using the Internet without human interaction. "Internet of Things" was popularized by Kevin Ashton, a British technology pioneer and co-founder of MIT's Auto-ID Center, in 1999. Ashton originally invented the term to express the value of linking goods using Radio-Frequency Identification (RFID) tags, eliminating the need for human involvement and automatically counts and monitors them. The recent creation of the Internet of Things (IoT) has popularized the idea of linking computers and servers all across the globe utilizing the Internet. This ushered in a new era of connectedness, in which everything may be linked at any time and from any location (Vashi *et al*., 2017) [35]. The sectors that embrace IoT are predicted to see a 22 percent increase in revenue (Kotha and Gupta 2018) [21]. Various Internet of Things (IoT) architectures have been developed to allow the use of heterogeneous devices in these systems. When you make the building design choices, think about the kind and quantity of devices you have, the application in use, and how much data you process and gather. The architecture in Figure 1 consists of three layers: the perception layer, the network layer, and the application layer.

- **Perception Layer:** This is the hardware layer of the IoT system. It is made up of sensors that gather environmental data and actuators that implement environment-altering actions. For example, a device such as an air conditioner's temperature controller exemplifies an actuator.

- **Network layer:** This is the transmission layer, which decides which network routes to use. Additionally, it is responsible for the data transmission and processing which occurs on the perception layer.

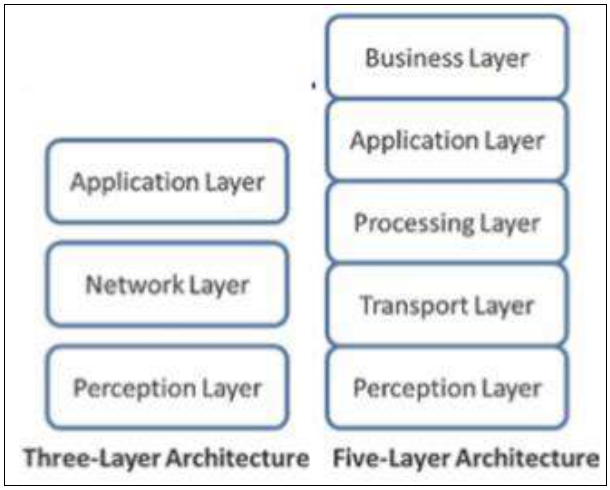

Fig 1: Network Layer

- **Application Layer:** This session provides end-users with application-specific services. It also serves as a way for users to be in touch with the IoT system. This is the most basic IoT architecture using a three-layer configuration. This architecture is becoming more wasteful as the system's data volume rises. This causes the five-layer model in Fig. 6.1 to be presented, in which the application and perception layers are combined with the following three levels (Sethi and Sarangi 2017) [33].

- **Transport Layer:** It also serves as a way for users to touch the IoT system. This is the most basic IoT architecture using a three-layer configuration. However, this architecture is becoming more wasteful as the system's data volume rises. This causes the five-layer model in Fig. 6.1 to be presented, in which the application and perception layers are combined with the following three levels (Sethi and Sarangi 2017) [33].

- **Processing Layer:** The middleware layer handles the bulk of the data stored and processed by the transport layer. Furthermore, it is responsible for pre-processing data for the application layer. Finally, this layer is responsible for administering and transmitting various services to the other levels. Using cloud computing, databases, and big data analytic technologies, this layer aids the operation of the whole system.

- **Business Layer:** The IoT application as a whole, as well as its business and revenue models, are encapsulated in this layer. It is also concerned with user privacy and security. The identical layer divides were presented in another design detailed in (Navani *et al*. 2017) [9], but with different names.

The architecture comprises four layers: objects, object abstractions, service management, and application development. Before the widespread use of cloud computing, the processing layer was built using cloud computing's enormous flexibility and scalability. A cloud database management system that consisted of five different levels was released in 2016.

(Alam *et al*., 2013) and task scheduler used by Malhotra *et al*. (2018) [26] (Malhotra *et al*. 2018) [26]. (As of this year, Ali *et al*.) because of the scarcity of energy in IoT devices, the authors of (Ali and Alam 2016) [2] suggested energy management methods for cloud computing environments. IoT devices gather important data and sharing it is critical. Cloud computing technologies and extensive data analysis are necessary for many platforms, as noted in Alam and Shakil (2016) [2]. (Khan *et al*. 2016, 2018, 2019a, b, c, d; Shakil *et al*. 2017) [17-19]. The recent increase in real-time applications that require low latency has necessitated a transition to processing architectures that utilize fog or edge computing. Data and processing occur in decentralized computing structures physically located between data sources and the cloud in fog computing paradigms. Time-sensitive IoT applications benefit from the reduced latency that fog computing offers. Since less data is uploaded to the cloud, its efficiency is also improved. Data processing can be done locally on the IoT device or a gateway device located near the IoT device in the edge computing paradigm.

2. Materials and Method

Machine learning approaches are meant to automatically profit from previous experience while acting in the future without intentional retraining. Supervised, unsupervised, and reinforcement learning are the three types of machine learning methods now accessible. On the other hand, artificial intelligence techniques have recently made important contributions to the progress of machine learning techniques. This paper further divides supervised learning, unsupervised learning, reinforcement learning, evolutionary computation, and fuzzy logic into several categories. This section describes the various machine learning algorithms and their most recent algorithms within IoT and WSNs.

2.1 Applied Supervised Learning

Both the input and intended output data are labelled for classification in supervised learning. This lays the groundwork for future data processing learning. The following are the main supervised learning algorithms:

1. This supervised learning methodology classifies a data sample based on neighbouring data samples' labels, as in the case of the K-Nearest Neighbor (K-NN). Most commonly, basic procedures (such as computing the Euclidean distance between IoT devices) determine the average measurements of the surrounding devices within a specific range. Although it is a simple computing method, it can be inaccurate when working with large data sets. k-NN is used in the Internet of Things for fault identification and data aggregation (Warriach and Tei 2017) [38]. (Li *et al*., 2014).
2. Support Vector Machine (SVM): Decision planes are used in SVM methods to determine decision boundaries. Because SVM supervised learning is so accurate, it is often used to identify harmful behaviour, resolve security problems in IoT and WSNs, and pinpoint a device's location, as seen in the following example: (Zidi *et al*. 2018).

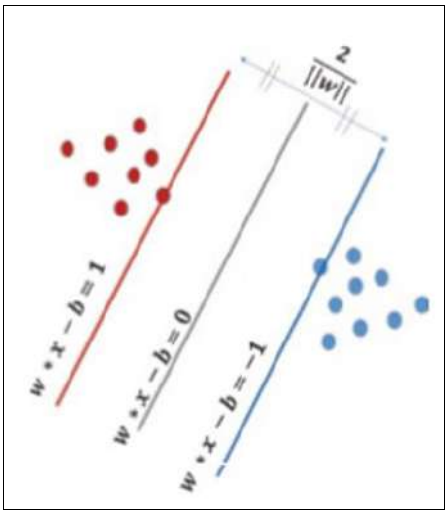

Fig 2: Support Vector Machine

3. Artificial Neural Network (ANN): An artificial neural network (ANN) uses artificial neurons connected in layers to imitate the functionalities of biological neurons. An artificial neuron uses distinct input data sets to generate diverse output data sets. The model of a neural network is shown in Figure 3. Computationally intensive ANNs can solve non-linear and complex problems, but not everyone has the necessary hardware. IoT localization (Banihashemian *et al*. 2018; El Assaf *et al*. 2016) [7, 10] improves neural network efficacy, detects malfunctioning nodes, and devises routes (Banihashemian *et al*. 2018; El Assaf *et al*. 2016) [7, 10]. In 2016, researchers reported (Chanak and Banerjee 2016) [8]. (Mehmood and colleagues, 2017) [27].
4. Bayesian Interface: Bayesian inference, unlike the bulk of machine learning algorithms, only needs a small amount of training data. By modifying probability distributions and minimizing overfitting, Bayesian algorithms effectively learn ambiguous perceptions. They do, however, need a previous understanding of the surroundings. Bayesian frameworks for defect identification, cluster head selection, and localization approaches (Wang *et al*. 2018; Guo *et al*. 2018) [36, 11].
5. Decision Tree (DT): A decision-support tool of this kind employs a tree-like paradigm of decision-making or categorization. DTs are generated by the use of a

series of if-then conditions. The random forest (RF) technique is used to improve DT accuracy. RF is a technique for building many classifiers in an ensemble decision tree. Classifiers are made up of one or more decision trees. In some applications, RF sensors are used in intrusion detection; in other cases, RF sensors are used for a wide variety of other purposes (Varsha *et al*., 2017).

2.2 An unguarded learning

Unsupervised learning methods are effective on datasets where there are no predetermined answers. These algorithms group the unlabeled data into clusters and use this information to reach conclusions. PCA shrinks the number of variables to a much smaller collection encompassing almost all of the original colossal set's information.

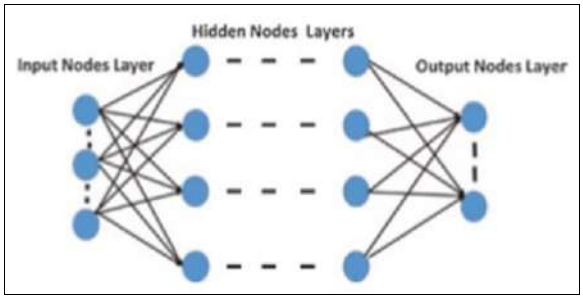

Fig 3: Neural Network Structure

PCA is used at the sensor or cluster head level to reduce IoT data dimensions. Communication cost lowers with PCA, which is excellent for data aggregation (Wang *et al*. 2019) [37]. Liu *et al*. (2017) say 2. The k-means algorithm is a technique for clustering data (Jain *et al*., 2018) [13]. At the outset, a selection of k centroids is randomly chosen. Once all remaining nodes have been allocated, the remaining nodes will form clusters around the centroid closest to them. Then, new centroids are calculated by averaging all the nodes in each cluster. Until convergence is obtained, the algorithm performs the preceding stages again and again. 3. A dimensionality reduction technique, as stated in Miljkovi (2017) [28], is referred to as a SOM. The primary difference between a SOM and an ART is that the latter (an ART) uses unsupervised learning to construct a low-dimensional representation of the input data known as a map, while the former (a SOM) utilizes supervised learning to build a discretized low-dimensional representation of the input data known as a map. SOMs are a great contender for clustering in the Internet of Things.

2.3 Agent-controlled training

The training set should include previous knowledge of the inputs and outputs for reinforcement learning (RL) to work. Machine learning is a fundamental approach whose principle is that an agent acquires knowledge and abilities by interacting with its environment and obtaining rewards for certain behaviours. If 6.5. RL algorithms have been used to develop routing protocols for the Internet of Things (IoT) and wireless sensor networks (WSNs) to save energy and boost network performance (Habib *et al*., 2018) [12]. Q-learning is a widely used reinforcement learning method. After initializing a Q table, the action AN is executed. Following that, a reward is calculated to update the Q table. The algorithm learns the action-value function Q (s, a) to determine how beneficial it is to do an action AN at a particular state. The action AN is first picked randomly until the Q table is formed; then, the best action is chosen.

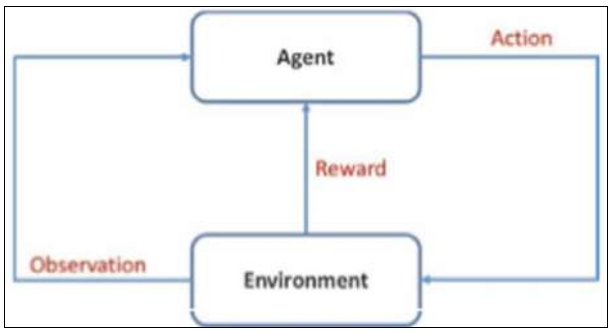

Fig 4: Reinforcement Learning Concept

3. Result and Discussion

While the fundamental operational concerns are directly related to how an IoT system operates, performance problems focus on improving the system's performance. The performance improvement needs include default detection, mitigation, congestion management, and high quality of service and security. How machine learning may be used to study performance issues

3.1 Allocation of Congestion Controls

Congestion has a detrimental effect on the performance of IoT applications by causing packet loss, increasing encountered delays, wasting the nodes' energy, and drastically degrading the fidelity of IoT applications. Therefore, congestion management in IoT and WSN increases network performance and decreases data transmission latency. As a result of this motivation, the authors proposed a congestion detection phase followed by a congestion monitoring period (Ali 2019) [2]. The technology identifies congestion by monitoring the rate of data loss. Congestion monitoring is essentially an ANN that learns about congestion situations to lessen and prevent them before they occur. When compared to the usual scenario of no congestion management, our strategy demonstrated a considerable improvement.

3.2 Fault Detection

The definition of the IoT system (Warriach and Tei 2017) [38]. The problems that result from a node failing because of physical damage, battery depletion, communication interference, or environmental interference all lead to new failures. A fault is the false detection of a condition or event in a particular space due to a defect. Faults may be grouped into the following categories:

- Offset fault: This issue arises when data consistently deviates from its intended value by a constant amount due to incorrect sensor module calibration.
- Gain fault: This kind occurs when the amount of change measured does not correlate with the projected value.
- Stuck-at faults: When practical information is constant, this occurs (zero-variance).
- Out-of-limitations fault: When detected data values go outside the limitations of usual functioning, this happens.

In Warriach and Tei (2017) [38], the subject of defect detection is revisited as a classification issue where incoming information is classified as usual or defective. Three machine learning methods were employed to achieve this goal: k-Nearest Neighbor, Support Vector Machine, and Naive Bayes. k-NN generates in the quickest possible time, followed by SVM, the fewest classification mistakes. The worst, though, was Nave Bayes. The authors of (Zidi *et al*. 2018) have highlighted some different faults and how they might be resolved. This was a random failure characterized as a temporary time-length instantaneous error when data is disturbed. These errors result in some high positive or negative peaks, which impact sensor data. Because these interruptions occur rapidly, they become more challenging to detect. The authors proposed an SVM classifier to detect mistakes with a 99% accuracy rating and instantly occurred. Enhanced SVM (ESVM) is advocated in (Javaid *et al*. 2019) [14] to develop conventional classifiers. The authors also used Enhanced KNN (EKNN) and Enhanced Extreme Learning Machine (ERELM) to increase their accuracy. Additionally, Noshad *et al*. (2019) [30] employed an RF technique and surpassed SVM and NN with their findings.

3.3 Sustainable Resource Management

Robust resource management systems that cut energy use and response time are needed to fulfil the important resource requirements of varied IoT applications. Since IoT system systems are dynamically functioning, RL is among the most suited machine learning techniques for IoT resource management, as indicated (Kumar and Krishna 2018). However, as the number of action pairs increases, RL complexity increases. Therefore, researchers integrated NN with RL (Chowdhury *et al*. 2019) to create a new Deep Reinforcement Learning methodology (DA-DRL). Time-division multiple access, Q-learning scheduling were studied further in (Zhang *et al*. 2019) [6] to improve real-time dependability (QS-TDMA).

3.4 Security

Due to the resource restrictions of IoT devices, it poses a severe problem to protect them from security assaults. Many solutions are available for cloud computing on IoT devices to ensure authentication (Kumari *et al*. 2018; Alam *et al*. 2015) [24, 1]. However, more than two-thirds of Internet of Things (IoT) devices now have significant security issues, as shown by (Williams *et al*. 2017) [39]. Therefore, it is becoming more necessary to use machine learning approaches to safeguard these networks from different safety attacks. This section will examine the five most common IoT security threats (Mamdouh *et al*., 2018).

1. Attacks of this nature are referred to as distributed denial of service (DDOS) assaults. They are characterized by the attackers flooding the system with excessive requests, exceeding the system's capability and bringing it to its knees.
2. Spoofing Attack: This is a sort of cyberattack. An attacker tries to mislead the system by masquerading as an authorized node to perform legitimate activities or disclose sensitive information.
3. A malware Attack: is a sort of cyber-attack when malicious software or malware performs operations on the operating system of a target, frequently without the consciousness of a victim.
4. The attacker tries to get superuser or root rights in this attack. This is done by using stolen identifiers or infections with malware.
5. Distant to Local (R2L): the attacker calls a real user to access the destination device from a remote device.

Distributed Denial of Service attacks is recognized by (Doshi *et al*. 2018) [9]. Information is gathered and organized for study. Packet size, inter-packet arrival, the protocol utilized, available bandwidth, and node/IP destination have all been established as criteria for distinguishing average IoT data from DDOS data. That is why these traditional techniques, such as Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), Artificial Neural Networks (ANN), and Random Forests, have been utilized. Such observations led to this conclusion. The best performance was observed for the Random Forest and the k-NN. This model, developed by Thamilarasu and Chawla (2019), uses machine learning and profound learning to build a deep neural network capable of identifying DDOS assaults with increased efficiency. In other words, the cloud traceback technique is used in combination with NN to detect DDOS attacks (Alam *et al*., 2015) [1]. The stages to successful spoofing attacks are shown in Figure 6.9. Machine learning methods are often utilized at the stage of feature recognition and assault detection. A k-means approach for disclosing features (from Lima Pinto *et al*. 2018) recommended a k-NN classification. In addition to two classifiers, PCA applies another technique (Pajauh *et al*. 2019): a Naive Bayes, followed by a k-NN classifier to reduce dimensions. This two-tier categorization guarantees that safety attacks are quickly detected and accurately detected by U2R and R2L. We have utilized random forestry and k-NN to approach malware detection as a classification problem (Pajouh *et al*., 2019) [31]. Yu and Tsai (2008) have shown the fascinating intrusion detection approach in which each sensor node has a detection agent for intrusions (IDA). IDAs do not collaborate because nodes cannot trust each other. The LIDC is in charge of extracting local features, including packet delivery and colliding rates, delays, neighbour counts, routing costs, and energy used.

Meanwhile, the intrusion detection component (PIDC) of the packet analyses packets that it suspects belong to an attacker to see whether there are signs of an attack and examines the RSS, sensor data arrival rate, and assailant packet transfer rate. In the following steps, the SLIPPER machine technique is employed. The recommendations were made to use the Generative Adversarial Networks (GANs) to protect the WSN and IoT platforms (Alshinina and Elleithy 2018) [4].

4. Concluding Remarks

Due to the specific characteristics of WSNs and IoT systems, we are obligated to use the correct tools and techniques to handle their obstacles and limitations. Supervised learning, unsupervised learning, reinforcement learning, evolutionary computation, and fuzzy logic are essential to this project. Regardless of the method used, all of these techniques can meet the needs of most cases. We saw many approaches to addressing key IoT concerns such as cluster formation, routing, and data aggregation in this paper. To study machine learning in a performance-related context, we first looked at how it may be used to handle such issues as congestion control, fault detection, resource management, and security. Finally, we'd like to make the

following observations:

- Aspects of performance rely heavily on supervised learning techniques. The algorithm must predict discrete values or categorize the input data in these situations, which are classed as classification tasks. Before beginning, it is required that you have a thorough understanding of machine learning, which is why supervised machine learning approaches are suitable in this instance.
- Instead of addressing performance difficulties, evolutionary techniques are used to solve operational concerns. Their goal is to introduce innovative behaviour and assess their effects by replicating ants to achieve a goal. As a consequence, evolutionary approaches are ineffective for modelling performance problems such as classification tasks. Fuzzy systems are increasingly being employed in IoT routing and node localization because they can cope with uncertainty and provide a broader range of truth.
- To handle resource management challenges, reinforcement learning is applied (Q-learning technique). Everything in the IoT changes continuously. Resource management requires a dynamic methodology continually engaged with its surroundings to have the requisite rapid answers. As a consequence, RL is a perfect match in this situation.

References

1. Alam M, Shakil KA, Javed MS, Ansari M. Ambreen: Detect and filter traffic attacks through cloud trace back and neural network. In International conference of parallel and distributed computing, 2015.
2. Ali SA, Alam M. A comparative study of task scheduling algorithms in the cloud computing environment. In 2nd international conference on contemporary computing and informatics (IC3I), 2016.
3. Ali SA, Affan M, Alam M. A study of effective cloud-based energy management systems. 9th International Cloud, Data Science, and Engineering Conference (Confluence), 2019.
4. Alshinina R, Elleithy K. An exact technique to deep learning in constructing network middleware of wireless sensors. Access IEEE 2018;6:29885-29898.
5. Arjunan S, Sujatha P. Lifetime maximization for the network of wireless sensors utilizing the uniform clustering based on fuzzy and the hybrid protocol-based ACO routing. Intelligence applications 2018;48(8):2229-2246.
6. Ayodele T. Intro to machine learning. New progress in machine learning in Y. Zhang (Ed.). Open Intech, 2010.
7. Banihashemian S, Adibnia F, Sarram M. The new localization approach, free of range and storage efficiency, uses neural networks in wireless sensor networks. Personal Communications Wireless 2018;98(1):1547-1568.
8. Chanak P, Banerjee I. Fuzzy rules-based, large-scale wireless sensor networks with flawed node categorization and management system. Application Expert Systems 2016;45(C):307-321.
9. Doshi R, Apthorpe N, Feamster N. Machine DDoS detection of things devices for the consumer internet. ALLXIV arXiv preprint 2018, 1804.04159.
10. El Assaf A, Zaidi S, Affes S, Kandil N. In the case of anisotropic signal attenuation, robust ANN-based WSN localization. Wireless Letters of IEEE 2016;5(5):504-507.
11. Guo Y, Sun B, Li N, Fang D. Bayesian variable inference counting and off-grid target location with defective information in wireless sensor networks. Communications transactions of the IEEE 2018;66(3):1273-1283.
12. Habib A, Arafat M, Moh S. Routing methods based on wireless sensor network enhancement learning: a comparative study. Dynamic and control systems advanced research journal. The archive of PHP? 6166 is the archive. The archive of PHP? 2018;(14):427-435.
13. Jain B, Brar G, Malhotra J. EKMT-k is a clustering technique for low energy consumption based on a minimum average distance from the base station for wireless sensor networks. Communication and data engineering networking, 2018.
14. Javaid A, Javaid A, Wadud Z, Saba T, Sheta O, Saleem M *et al*. Machine learning and defect detection strategies in wireless sensor networks to increase belief functional decision fusion. Sensors, 19, paragraph 2019;6:1334.
15. Khan S, Shakil KA, Alam M. Education Intelligence: The Indian education system is subject to cloud-based Big Data Analysis. 2nd international conference on modern computing and computer technology (IC3I), 2016.
16. Khan S, Shakil KA, Ali SA, Alam M. To develop a general Big Data Framework as a Service. In: IEEE International Conference on Engineering Research, 2018.
17. Khan S, Shakil KA, Alam M. PABED - a data analysis tool for extensive education. International Industrial Technology Conference at the 20th IEEE, 2019a.
18. Khan S, Liu X, Ara Shakil K, Alam M. Big data technology-Enabled analytical solution for higher education system quality evaluation. Advanced Science and Applications International Journal (IJACSA), 10 10 (6). Scopus/ESCI, 2019b.
19. Khan S, Arshad Ali S, Hasan N, Ara Shakil K, Alam M. Cloud science: challenges and promises for the future. Geospatial Analytics Cloud Computing, 2019c, 1–28.
20. Khan S, Shakil KA, Alam M. Cloud-based big data computing: challenges and prospects. Future Networks: architecture, technology, and execution, 2019d.
21. Kotha H, Gupta V. Application for IoT - A survey. Engineering & Technology International Journal 2018;7:891-896.
22. Kumar A. A cooperative, scalable, and secure, hybrid fuzzy system-based location system for Wireless Sensor Networks (IMN) 2018;10:51-68.
23. Kumar T, Krishna P. Modelling the power of IoT sensors via strengthening study. Advanced Intelligence International Journal Paradigms 2018;10(1-2):3.
24. Kumari A, Abbasi MY, Kumar V, Alam M. Cryptanalysis of secure authentication based on the IoT and cloud server elliptic curve encryption. International Conference on Computing, Communication Control and Networking Advances at IEEE (ICACCCN) 2018.
25. Li Y, Parker L. Close neighbour imputation in wireless sensing networks with spatial-temporal correlations. Merger Information 2014;15:64-79.
26. Malhotra S, Doja MN, Alam B, Alam M. A widespread

cloud database management system query processing method. Extensive data analysis. Singapore: Springer, Singapore 2018, 641-648.
27. Mehmood A, Lv Z, Lloret J, Umar M. ELDC: An energy-efficient and resilient routing system based on the artificial neural network to detect pollution in WSNs. Emerging Computing IEEE Transactions, 2017,1–1. https://ieeexplore.ieee.org/abstract/doc/7859382/quotes#quotes.
28. Miljković D. A short examination of self-organized maps. IEEE's IT, electronics, and microelectronics international conference worldwide (MIPRO) 2017.
29. Navani D, Jain S, Nehra M. IoT: a study of architectural aspects. The Internet of Things. 13th Signal-Image Technology & Internet-based Systems International Conference (SITIS), 2017.
30. Noshad Z, Javaid N, Saba T, Wadud Z, Saleem M, Alzahrani M. Fault detection via random forest classifier in wireless sensor networks. Cryptography 2019;19(6):1568.
31. Pajouh H, Javidan R, Khayami R, Dehghantanha A, Choo R. A reduction in two layers and a dual-level classification model to detect abnormal incursion in IoT networks. IEEE Emerging Computing Themes Transactions 2019;7(2):314-323.
32. Sam S. The Internet of linked devices Things will treble to more than 46 billion gadgets by 2021—research in Juniper, 2016.
33. Sethi P, Sarangi S. Things' web: architectures, protocols, and apps. Computer Engineering and Electrical Diary 2017;1:1-25.
34. Van der Windmills R. In 2017, Gartner believed it is set to use 8.4 billion related items, up 31% from 2016. Gather Research. - Gather Research, 2017.
35. Vashi S, Ram J, Modi J, Verma S, Prakash C. Things Internet (IoT): vision, architecture, and security problems. Things Internet. IEEE International Social, Mobile, Analytics and Cloud IoT Conference International (I-SMAC), 2017.
36. Wang J, Cao J, Sherratt R, Park J. An enhanced colony-based optimization technique for wireless sensor networks with mobile sink. The supercomputing newspaper 2018;74:6633-6645.
37. Wang J, Gao Y, Liu W, Sangaiah A, Kim H. An enhanced routing schema for heterogeneous wireless sensors with specific clustering utilizing PSO algorithm. Receiver 2019;19(3):671.
38. Warriach E, Tei K. Comparative examination of machine learning techniques for detecting errors in networks of wireless sensors. Sensor Networks International Journal 2017;24(1):1-13.
39. Williams R, McMahon E, Samtani S, Patton M, Chen H. Identifying consumer Internet of Things (IoT) vulnerabilities: a methodology that can be scaled up. At the IEEE International IT and Security Conference (ISI), Detection of failure in SVM classifier wireless sensor networks. Journal of IEEE Sensors 2017;18(1):340–347.