Scientific Research Publishing

Advances in Internet of Things, 2021, 11, 153-174
https://www.scirp.org/journal/ait
ISSN Online: 2161-6825
ISSN Print: 2161-6817

A Review of Identity Methods of Internet of Things (IOT)

Sana Abdelaziz Bkheet[1], Johnson I. Agbinya[2]

[1]Faculty of Computer Science and Information Technology, Sudan University of Science and Technology (SUST), Khartoum, Sudan
[2]Melbourne Institute of Technology, Australia School of Information Technology and Engineering, Melbourne, Australia
Email: sanaaziz569@gmail.com, jagbinya@mit.edu.au

How to cite this paper: Bkheet, S.A. and Agbinya, J.I. (2021) A Review of Identity Methods of Internet of Things (IOT). *Advances in Internet of Things*, **11**, 153-174.
https://doi.org/10.4236/ait.2021.114011

Received: August 16, 2021
Accepted: October 10, 2021
Published: October 13, 2021

Abstract

The Internet of Things (IOT) is a recent technology originating from the field of sensor networks. It has received significant attention because it is involved in most aspects of our daily lives. The IOT vision makes objects of various kinds become part of the Internet by assigning each object a unique identifier, enabling objects to communicate with each other in the same or different environments. IOT can collect, process, and exchange data via a data communication network. There are many methods for identifying objects; some have existed since the beginning of IOT innovation, such as Radio Frequency Identification (RFID), Barcode/2D code, IP address, Electronic Product Codes (EPC), etc. Continuous development in IOT domain and the large number of objects connected to the Internet daily require an improved identification method to cope with the rapid development in this field. Many modern methods have been proposed recently, based on various technologies such as computer vision, fingerprinting, and machine learning. This paper introduces an overview of IOT and discusses its fundamental elements; it mainly focuses on identification of IOT which is considered the main part that the IOT systems rely on. The paper discusses the existing identification methods for IOT. Moreover, it provides a review of the modern identification methods proposed in recent literature.

Keywords

IOT, IOT Elements, Wireless Sensor Network (WSN), Identification Methods

1. Introduction

The Internet has been rapidly growing in the last few decades. At first, the Internet connected computing devices. Today, the Internet can connect heterogeneous devices or objects, creating a new concept that refers to tens of billions of

interconnected physical objects, or "things" known as smart objects that are typically equipped with sensors or actuators, tiny microprocessors, communication interfaces, and a power source. This concept is commonly known as the Internet of Things (IOT). IOT devices communicate in various contexts. They need to authenticate each other to know that they talk to the particular party. Authentication typically involves identification in different ways, such as the use of unique numbers, names, or tokens [1] [2] [3] [4] [5].

1.1. The Elements of IOT

Creating an IOT environment requires defining the IOT element that helps clarify IOT functionality. IOT mainly consists of six elements needed to provide the IOT functionality [6]: identification, sensing, communication, computations, services, and semantics, as illustrated in **Figure 1**.

1.1.1. Identification

Identification, the first requirement in IOT elements, is considered proof of identity information for each object in the IOT world. Identity is usually used to identify a particular person, device, or entity. Moreover, it is considered a key factor in creating a connection or relationship between individuals and critical for IOT system success. It enables us to identify billions of heterogeneous objects and manage remote objects through the Internet.

Identification also links objects to information associated with the particular object that can be retrieved from a server. It enables the object to communicate with other objects through the Internet in the same or different scope. There should be a way to coordinate the identities of all IOT objects in the scope to allow secure inter-object communication. Identity management is required for three main parties: the user, object identities, and relationships, depending on

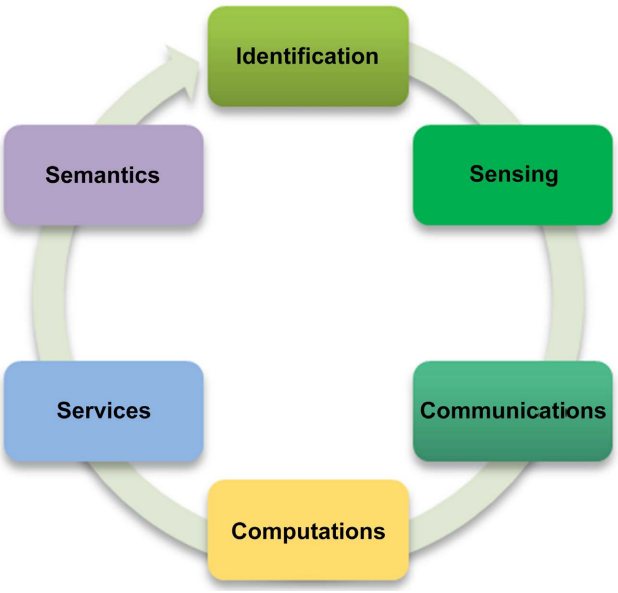

Figure 1. IOT elements.

the certain principles that applies to object identity. It must also deal with unique challenges in the IOT model [1] [2] [3] [4] [5].

On the one hand, identification is significant for the IOT to name and match services with their scope, the challenges regarding applying each object with a unique identity, and representation and storing of exchanged information. On the other hand, addressing the IOT objects is necessary to differentiate between object ID or name and its address, referring to the object address within a communication network. There are addressing methods for IOT objects like IPv4, IPv6, and 6LoWPAN addresses, as well as many former identification methods such as Radio Frequency Identification (RFID), Bluetooth, Barcode/2D code, Near Field Communication (NFC), Electronic product codes (EPC), IP address, etc. Identification methods give each object within the network a clear and unique identity [2] [6] [7].

1.1.2. Sensing

Sensing is gathering data from the environment and then sending it to storage and use media, such as a database, data warehouse, and cloud. Many sensing devices gather data, like actuators, RFID tags, smart sensors, wearable sensors, etc.

IOT devices' limited data storage capabilities, which make the processing of sensed data, are very important. The processed data is base on the requirement to take appropriate action [8] [9] [10].

1.1.3. Communication

Connecting a huge number of heterogeneous objects and exchanging information to provide some service is an important issue and requires communication technology. Communication in IOT is an essential part of object connection, but communication is permanently restricted by object characteristics, such as battery life or limited range of data transmission.

There are various communication technologies used for the IOT, such as Wi-Fi, Bluetooth, RFID, NFC, IEEE 802.15.4, Z-wave, zigbee and Long Term Evolution (LTE) [8] [9] [10].

1.1.4. Computations

In the computation step, the information collected from various objects in IOT applications, must go through a processing procedure. The information is filtered to specify the useful information and remove unnecessary one. Several hardware and software platforms are involved in performing this task, such as: Arduino, Raspberry Pi, Friendly ARM, Intel Galileo, Beagle Bone, WiSense, Mule, etc., and software like: Tiny OS, Lite OS, Android, etc. These operating systems play an important role in processing, and also offer light weight OS that is suitable for designing IOT environments. Furthermore, cloud is considered as important computational part of the IOT. That it provides facilities for smart objects to send their data to the cloud, allows big data to be processed in real-time, and enables end-users to benefit from the knowledge extracted from the collected big data [8] [10].

1.1.5. Services

IOT applications can mainly provide four types of services; Identity related services, Information aggregation services, Collaborative Aware services, and Ubiquitous services. The Identity related services are concerned with object identity information, whereas Information aggregation is used to collect, summarize, and process all the information from objects and send it back to the application. Moreover, Collaborative Aware services are used to turn the collected information into a decision and send appropriate responses to the devices. The last service is Ubiquitous services, which are responsible for providing Collaborative-Aware services immediately to anyone at any time and place [8] [9] [10].

1.1.6. Semantics

Semantics is considered as the brain of IOT. It is used to extract knowledge smartly from devices to take appropriate decisions in order to provide the desired services. It discovers and uses resources and modeling information. The Resource Description Framework (RFD) and the Web Ontology Language (OWL) are examples of Semantic Web technologies [8] [9] [10].

1.2. Wireless Sensor Network (WSN)

Wireless sensor network (WSN) is one of the rapidly growing sections in networking today [11]. It is a self-configured wireless network consisting of independent devices which are spatially distributed [12]. Formally, a WSN can be defined simply as a network of low-size and low complexity devices known as nodes that use wireless communication link to sense the environment and send the data gathered from the monitored environment to control unit for further processing and decisions. Moreover, the collected data is forwarded via multiple hop relaying, to a sink or base station, which is considered as an interface between users and the network, the sink can use the data locally, or is connected to other networks (e.g., the Internet) via a gateway [13] [14].

Typically a wireless sensor network contains thousands of sensor nodes, which can communicate among themselves using radio signals, so it is equipped with sensing and computing devices, radio transceivers and power components. All the nodes in a wireless sensor network are resource constrained: they have limited storage capacity, processing speed, and communication bandwidth [13].

WSN usually uses sensors for monitoring physical or environmental conditions, such as motion, temperature, vibration, pressure, sound, or pollutants. Furthermore, sensors can observe other phenomena, not just ambient conditions. These sensors are deployed widely in many remote sensing applications, such as infrastructure monitoring, habitat monitoring, intrusion detection, target tracking and surveillance, oceanography, structural health monitoring, biomedical health monitoring, precision agriculture, and hazardous environment exploration and seismic sensing [12] [13] [14].

The diversity of fields and environments where the WSN can be implemented makes it necessary to have enough knowledge of communication and signal

processing, hardware technologies, embedded system design, and software engineering [14]. When the need arises to deploy WSN in any environment, a wireless sensor network is considered a subpart of IOT and one of its most important elements [12].

This paper aims to present the existing object identification methods and provide a review of the modern identification methods proposed within the last decade to provide a basis for new approach for identifying IOT objects. It is organized as follows: Section 1 presents a brief introduction about IOT, Wireless sensor Network, and the IOT elements; Section 2 provides an overview of IP addressing methods; Section 3 discusses the prior object identification methods; Section 4 contains a review of some recent methods that have been proposed in the last decade. Section 5 provides an introduction about fuzzy logic, machine learning, and deep learning, which helps to choose the best identification method for IOT objects. Finally, Section 6 concludes the paper.

2. IP Addressing Methods in IOT

2.1. IP Address

The Internet Protocol (IP), developed in the 1970s, is considered the prime communications protocol in the Internet protocol suite for relaying data across a network. There are two main versions of IP in use: IPv4 and IPv6. Each one of them defines an IP address in a different way. IPv4 provides about 4.3 billion addresses, while IPv6 will efficiently provide 85,000 trillion addresses [12]. In the present day, these two versions of IP are widely used to connect different networks together [15].

(IPSO) IP for smart objects (IPSO) has promoted IPv6 as the main solution for accessing and communicating with all kinds of smart objects. Using the IP address to identify objects will cause difficulties when an object or device is moving. In this case, the IP address cannot identify the object conclusively, even if the roaming function is enabled. The roaming function is based on a unique device identity and not the IP. Therefore there is a need to apply a unique object/device identity instead of IP addresses to cope with roaming situations [16].

2.2. IEEE 802.15.4

IOT applies the IEEE 802.15.4 protocol because it has low data rates, low cost, low power consumption, and high message throughput. It specifies a sub-layer for MAC (Media Access Control) and a physical layer for low-rate wireless private area networks (LR-WPAN). This protocol can handle many nodes with reliable communication, and it can operate on different platforms. Moreover, it grantees a high level of security, encryption, and authentication services [15].

2.3. IPv6 and 6LoWPAN

To enable any objects to be connected to the Internet, they should have an address so that they can be detected and monitored, especially in IOT environment

which consists of a huge number of heterogeneous objects with various resource constraints, and the number of these objects is in continuous growth. Therefore, the IOT implementation requires a suitable communication protocol that can cope with this complex situation [17] [18]. In this regard, IPv6 founds to be more reliable and useful as compared to IPv4 in assigning addresses to devices, routing in networks, translation of network address, support of configuration of protocol, and security of information and data [15].

The Internet Protocol Version-6 (IPv6) is the successor to IPv4. It was published by the Internet Engineering Task Force. IPv6 provides a unique address to each device connected to the network. Moreover, it has unique identities, auto configurations of addressing and high numbers of addressing nodes. It supports 2^{128} bits (approximately 3.4×10^{38}) unique addresses, has a high capacity in addressing and can connect a huge number of devices to the Internet [17] [19] [20].

During the last decade, embedded systems and sensor networks have been widely extended, and experienced rapid growth in using wireless technologies. IPv6 is needed to support such Wireless technologies like WSN, which is considered one of the fastest growing segments in ubiquitous networking since it consists of huge numbers of nodes, and these networks may be connected to others via the Internet. Moreover, WSN involves many constraints such as limited memory, limited processing capability, and short battery life. That makes it difficult to support IPv6 and requires a new communication protocol that can efficiently manage this condition. For this reason 6LoWPAN was designed [11] [18] [19].

6LoWPAN is a combination of IPv6 and Low power Wireless Personal Area Network (WPAN), integrated with IEEE 802.15.4 standard, taking into account the limited bandwidth, memory and energy resources. It is essentially developed to operate in a network environment with huge number of embedded sensor devices over low data-rate, limited power and relaxed throughput requirements. 6LoWPAN enables the Wireless Embedded Internet by simplifying IPv6 functionality, and specifying very compact header formats. It is characterized by short range, low bit rate, low power, low memory usage and low cost [11] [18] [21].

3. The Prior Identification Methods

All objects in the IOT environment must be identified in some way. Thus, each object must have a unique identity to connect with other objects and exchange information within the same or different domain. This section will mention some of the prior identification methods in use to identify IOT objects.

3.1. Radio Frequency Identification (RFID)

RFID technology first appeared in 1945. It was one of the important developments in the embedded communication field and enabled the design of micro-

chips for wireless data communication. It uses radio waves to identify and track anything they are attached to automatically. RFID technology is considered a means of collecting data about a certain element without seeing or touching the data carrier. The main components of RFID are tag, reader, antenna, access controller, software, and server. Moreover, it is classified into three main categories based on the method of power supply provider in Tags: Active RFID, Passive RFID, and Semi Passive RFID [12] [22] [23] [24] [25].

RFID System

The RFID system consists of tags, readers, and applications, as illustrated in Figure 2. The tag is also known as transponders (transmitter/responder), a microchip connected with an antenna used to transmit and receive radio waves for communication purposes. The RFID tag can be attached to an object as the identifier of the object. It could be either active or passive. Active tags are partly or fully battery-powered and can communicate with other tags. Passive tags have no internal power source. They are powered up by the tag reader.

The RFID reader is made up of a radio frequency interface module and control unit; it uses radio waves to communicate with the RFID tag. RFID reader is also known as transceiver or interrogator (transmitter/receiver). Its main task is to activate the tags, structure the communication sequence with the tag, and transfer data between the tags and application software.

Application system is known as data processing system, which can be an application or database. Its main function is to initiates all readers and tags activities.

RFID provides a quick, reliable, and flexible radio frequency (RF) way for electronically detecting, tracking, and controlling various things.

The RFID system generally covers three main aspects: monitoring, tracking, and supervising [25].

In the RFID system, it is necessary to calculate the read range that is considered one of the main features that affect the performance. The following equation

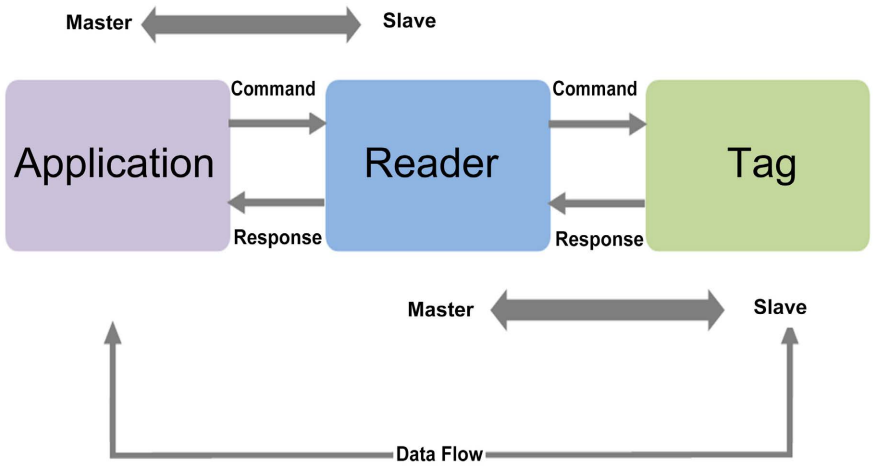

Figure 2. Typical RFID system.

shows that the RFID system with RTD_{max} is the distance between the reader and tag antenna, so the read-range can be calculated using Friis' uplink model in Equation (1)

$$RTD_{max} = \frac{\lambda}{4\pi}\sqrt{\frac{P_t G_t G_r}{P_{th}}} \quad (1)$$

where λ is the wavelength calculated using the speed of light c = 3×10^8 m/s divided by frequency f = 920 MHz. For antenna, P_t, and G_t are respectively, reader's transmitted power transmission gain, and the tag's antenna gain, G_r [26]. P_{th} designates the distance into which the reader radiates the power.

RFID has been widely used in many areas and applications such as logistics, pharmaceutical production, health care, passport and airport luggage tracking, toll system, retailing, supply chain management, identification, and access control. It was used for the first time in the Second World War in Britain to identify a friend or enemy. In 1999, RFID was founded at the Auto-ID center at MIT.

RFID technology is considered one of the main technologies in IOT. It plays an important role in solving identification problems of objects. It has great control over IOT, which is now largely used for identifying, tracking, monitoring objects, animals, and people. However, it transmits the identity of an object or person wirelessly using radio waves in the form of a serial number/Id. Identification technologies such as RFID are fundamental to the implementation of the IOT because they enable objects to be connected with their virtual identity on the Internet, besides the ability to label and tag every interconnected objects [4] [12] [24] [27] [28] [29].

3.2. Barcode/2D Code

A bar code is an optical representation of machine-readable labels attached to items that record data related to the item. It is widely used in stores to provide product information, such as product name, manufacture date, and price. This information is captured by a mobile phone camera encoded in the form of numbers and letters with a combination of bars and spaces of varying width. It can be decoded with a reader to obtain the recorded information. Usually, the reader is a laser scanner, but sometimes cameras can be used. There are three types of barcodes of Alpha Numeric, Numeric, and 2 Dimensional Barcodes (2D code) [12] [23].

3.3. Electronic Product Codes (EPC)

EPC codes are an identification standard developed by GS1 AISBL in a uniform resource identifier form. They are used in IOT field to identify and capture static information of objects such as name and manufacture. The main advantage of EPC code is that it provides unique identification of a static device object referring to a product. The disadvantages of EPC model are that different EPCs may encode the same product in heterogeneous codes, which could be confusing [16].

4. The Modern Identification Methods

This section provides a review of the modern IOT object identification methods that have been proposed recently in the last seven years.

4.1. Identification Using the Fingerprints of Things

The process of collecting device or object information to describe it is known as device/object fingerprinting. It aims to extract different types of information about devices, such as software, operating system, and hardware components, to create a unique signature called a fingerprint [30].

The fingerprint is an identification technology that implements individual recognition and authentication. That can be achieved by various methods, like capturing images of the surface pattern specific to each individual, in which image is taken under specific lighting conditions, and it is magnified using a microscope. The surface irregularities of each component have a slightly different pattern from those of the other components. In this method, each image is registered in a database [31]. Another method presented by the author in [30] has provided a feature-based device identification technique, in which the device features are extracted from a sequence of packets during the initial startup of a device, and then machine learning is used for classification [30]. Sandhya Aneja *et al.*, in [32] proposed a Device Fingerprinting (DFP), a device identification method based on the information taken from the packets, the information that allows the device to communicate over a network. The authors in this work implemented DFP using Inter Arrival Time (IAT). IAT is the interval time between two consecutive packets. This is considered unique because of the different hardware and the software platform used for the device. DFP is used to create a unique device identity without any of the assigned identities: IP address, MAC address, or International Mobile Equipment Identity (IMEI) number [32]. The work in [33] presented a device identification methodology based on device behavioral fingerprinting, which is approximated using features extracted from the device's network traffic. Multiple machine learning classifiers are used for feature classification, like k-nearest-neighbors (kNN), Decision tree and Majority voting. Then trained machine learning models are used for extracting device features, which can be used to detect similar device types. The final result of this work shows that the fingerprinting device categories can be used for identifying different device types with a similar functionality [33].

The researchers, in [34] have presented a novel and robust device-specific identifier called IOT-ID, derived based on Physically Unclonable Functions (PUFs), which mainly gives each integrated circuit a unique "fingerprint". The (PUF) acts as the basic building block for IOT-ID that is constructed by combining features from a clock and ADC PUFs, viz, $\text{clock}_{\text{count}}$, $\text{ADC}_{\text{signal}}$, and ADC_{diff}. Thus, IOT-ID represented as:

$$\text{IOT-ID} = \left\langle \text{clock}_{\text{count}}, \text{ADC}_{\text{signal}}, \text{ADC}_{\text{diff}} \right\rangle \quad (2)$$

The IOT-ID, first calculates the clock oscillator PUF, which is needed for each microcontroller to determine the speed with which the microcontroller operates, but due to variations in the manufacturing process of clock oscillators, the number of clock cycles counted for a specific time period with one clock oscillator varies from one another. We have two clocks, clock1 and clock2, for a certain time "t", if M is the number of clock cycles counted by clock1 and N is the number of clock cycles counted by clock2, will be calculated by:

$$M * \text{clock1} = N * \text{clock2} \Rightarrow N = M * \text{clock1}/\text{clock2} \tag{3}$$

Equation (3) is used to create a PUF for a clock oscillator by aggregating the clock cycle count values of clock2 and clock1 to arrive at the total clock cycle count ($\text{clock}_{\text{count}}$) calculated as the sum of clock cycles:

$$\text{clock}_{\text{count}} = \sum_{k=1}^{N} \text{cycle}_k \tag{4}$$

Second, the IOT-ID calculates the Analog-to-digital converter (ADC) PUF, which is included in every IOT device microcontroller. ADCs generally support both single and differential modes, where ($\text{ADC}_{\text{signal}}$) is the expected output from the voltage difference between the input voltage (V_{in}) and ground *w*. Which is calculated by:

$$\text{ADC}_{\text{signal}} = \sum_{K=1}^{N} \left(\frac{V_{\text{in}}}{V_{\text{ref}}} * 2^{\text{res}} \right)_K \tag{5}$$

res is the resolution supported by ADC, and V_{ref} can be either connected to an internal or external reference or to the device power supply in an IOT device. The (ADC_{diff}) is the voltage difference between two pins (V_{p1} & V_{p2}) which defined by:

$$\text{ADC}_{\text{diff}} = \sum_{K=1}^{N} \left(\frac{V_{p1} - V_{p2}}{V_{\text{ref}}} * 2^{\text{res}-1} \right)_K \tag{6}$$

Combining all these components together enables IOT-ID to be robust and act as a device-specific identifier. Moreover, they are implemented as a two stages edge machine learning (ML) model, which is first used to gather and store the features of IOT-ID for each instance, then IOT-ID had been trained for all devices to identify the device instance accurately. Furthermore, a new IOT-ID is then compared with the trained model to identify the device [34].

4.2. Identification Using Computer Vision

Computer vision is a scientific field that makes a computer gain a level of understanding of digital images or videos. It contains methods for acquiring, analyzing, and processing the digital images. In which the artificial systems are used to extract information from images. This information can be in many forms. For example, video sequences have views from multiple cameras.

Various computer vision methods solve real-world problems. These methods are identification, detecting events, computer-human interaction, object recog-

nition, object detection, object classification, and object tracking.

Computer vision consists of three main parts: the data acquisition part, the representation of data, and a decision part [35].

Authors in [36] have proposed a work that combines computer vision, deep learning, and IOT. They use U-Nets for semantic segmentation, which is an image processing technique used to associate the pixels of an image to a class label, which can help identify separate objects.

In this work, U-Nets architecture had been used to analyze 500 × 200 RGB images extracted from a satellite view of a crop area in an agriculture field. The feature is extracted by Histogram of Oriented Gradients (HOG), a common feature extraction technique implemented to classify and identify images. Besides applying four various classification algorithms, Logistic Regression, Support Vector Machines (SVM), K-Nearest Neighbors KNN, and Naive Bayes are used. The performance of these algorithms is compared to the same dataset to specify the best technique to solve the problem.

Here, an IOT system is used to identify fire initiation and record the temperature and humidity variations for further analyses [36].

4.3. Identification Using Machine Learning Methods

Machine learning (ML) is a branch of artificial intelligence (AI) that was introduced in the late 1950s. It improved rapidly and is now a powerful technique used extensively for a wide range of tasks, including classification, regression and density estimation in various application areas, such as computer vision, speech recognition, bioinformatics, spam detection, and fraud detection.

Many ML algorithms can be implemented with IOT systems to make them more efficient and scalable, such as SVM, Reinforcement learning, and Neural Networks [37].

Many researchers have adopted ML technologies to their work in various computing domains. Examples include, the research paper provided by authors in [38] which applied Random Forest and Supervised Machine Learning algorithm to IOT device features extracted from network traffic data of individual devices. These traffic data was used to identify IOT device types from a list containing many devices. The white list used here ensures that only authorized IOT devices can connect to the network. They are manually labeled network traffic data from 17 distinct IOT devices, representing nine types of IOT devices to train and evaluate multi-class classifiers [38]. Another work presented in [39] has applied ML on network traffic data generated by various devices connected to a network to identify IOT devices accurately. The authors have collected and labeled network traffic data from nine specific devices, PCs, and Smartphones to train and evaluate the classifier. They trained a multi-stage meta classifier using supervised learning, which consists of two stages. The first one is to distinguish between traffic data generated by IOT and non-IOT devices. The second stage links each IOT device with a specific IOT device class. They have proved that

IOT devices can be identified based on characteristics of the network traffic data they generate [39].

5. Review of Fuzzy Logic, Machine Learning and Deep Learning Use in IOT Identification

This section provides an introduction about fuzzy logic, machine learning, deep learning and neural Network, in order to find an appropriate method that fits the requirements of identifying IOT objects. Furthermore, the relevant related work in various fields and in IOT platform will also be discussed.

5.1. Fuzzy Logic

Fuzzy Logic was proposed by Lotfi Zadeh in the 1960s. The idea of fuzzy logic is essentially based on membership function which becomes the backbone of fuzzy set theory. Fuzzy logic was improved to solve problems that classical logic (binary logic) cannot address, such as contexts that need to deal with multiple values not only (0 or 1), which requires to make a decision by considering more information. In such a case these variable are usually known as linguistic variables and they can be represented by characters like "distance" whose values could be "short", "very short", "long", "very long", and so on. With fuzzy logic the answer to the same question will differ according to the case such as answering the question of how big a building is? The answer could be kind of fuzzy, such that the person who lives in a village, a 5 floors building could be big, but for a person who lives in Chicago, the same building will be considered very small.

Fuzzy logic plays an important role in decision making but will not be able to work in inference rules task where prior knowledge is required [40] [41] [42].

Fuzzy logic can give an accurate result, if it is combined with other methods such as Artificial Neural network, although it will never give 100% accuracy result. One of the best accuracy results was 80%, which was achieved by the work in [43] which combines fuzzy logic and neural network to develop an algorithm that was used to track and predict object location when it goes offline and becomes unable to send reports about its location. The algorithm works by recording history of movement of the object, then use the recorded data to estimate and get the future object location [43].

The Use of Fuzzy Logic in IOT Platform

Fuzzy logic has been implemented in various IOT environments such as smart buildings; basically for security purpose, surveillance and alarm systems that always aim to save lives and property from risk. Like in the research paper [41], a fuzzy logic based Fire Monitoring and Warning System (FMWS) for smart buildings, was created to early detect true-fire existence, which works by monitoring and detecting the true fire incident then notify the owner to take suitable action in order to stop fire. The proposed fuzzy logic system uses multiple sensors (e.g: temperature sensor, flame sensor) to collect the required information

based on this information an accurate result that shows the true existence of fire is produced this result will also help to reduce false alarms [41]. Also in [42] fuzzy logic has been proposed to control the indoor temperature based on reading of outdoor temperature and humidity. The outdoor data is obtained with the aid of many devices, which will also help in analyses of the gathered data. The temperature monitoring system will help in adapting the indoor locations of the smart cities in order to make it more comfortable for people who stay there [42]. In context of home security which is considered as a prime concern for home owners, a fuzzy smart home control system (SHCS) is proposed in [44], that gives the home owner the ability of remotely controlling the home applications based on Internet of Things (IOT) with the improvement of solar charger, the system supports many devices like lamps, speed-controlled fan, window blind and security gate. By the end of the system two different classifiers were selected in order to measure the accuracy of the fuzzy system and the results shows that the best accuracy achieved is equal 81% [44]. An intelligent health care system is proposed in [40] that use fuzzy logic and IOT to help people who live in remote areas to know whether they are suffering from serious health conditions and take appropriate action accordingly by contact the nearest hospital. The system takes the necessary information from three different sensors (body temperature sensor, pulse rate sensor, and heartbeat rate sensor) the collected data are managed and transmitted to the fuzzy logic system via communication and network devices to determine the patient condition and make a decision to take the suitable action. This system has been combined with neural networks to create a fuzzy neural network, which enhance the system work and achieves the best accuracy results [40].

The above introduction of fuzzy logic and its related work shows that the use of fuzzy logic will never give 100% accuracy, so we conclude that fuzzy logic is not suitable for identification of IOT objects because identification must be very accurate and specific.

5.2. Machine Learning (ML)

Machine learning (ML) is one of the most impressive fields in computer science. It was introduced in the fifties in the past century as a subfield of artificial intelligence. ML gets received great attention because it has the ability to construct systems that capable of learning from previous experience or data.

Machine learning is concerned with analyzing large collection of data, which makes it to be implemented widely in various areas, like: pattern recognition, spam filtering, handwriting recognition, activity detection, and it has frequently used for smart data analysis. ML is also data driven and general in nature so it can be used to make a decision in many general tasks.

The implementation of a ML algorithm mainly consists of two phases: training and testing. In the training phase, a set of input data named a training set is adapted to build a model that helps in making a decision to solve a particular problem. The produced output from the model will be tested by matching it with

the current input in testing phase.

ML is ideal for solving three major types of problems:

1) Classification: is the separation of the problem into set of associated samples which represents all the possible categories (classes) related to the problem. An example of ML classification task is like, specifying an e-mail message is spam or not, determining whether an object is a star, a galaxy, or a quasar. Other applications include digit and speech recognition, identity fraud detection, etc.

All the mentioned problems can be solved by using the following algorithms Support Vector Machine, Nearest Neighbor, Random Forest, and many others.

2) Regression: is the evaluation of the relationship among dependent variables from one or more independent variables. For example: weather forecasting, estimating life experience, predicting the cost of a house, and prediction of population growth. Such regression problems can be solved by using algorithms like Random Forest or Linear Regression.

3) Clustering: is the dividing of inputs into groups (clusters), which are mainly used to distinguish between the input features of the same objects, for example: among distant galaxies, specifying which features or collection of attributes are most important in distinguishing between galaxies. Another example, determining the main features that separate customer segments from each other to be treated with different privileges [35] [45] [46] [47] [48] [49].

5.2.1. The Learning Types

The learning algorithms are divided into four main categories: supervised, unsupervised, semi supervised and reinforcement as shown in **Figure 3**.

In supervised learning the input vectors (labels) and output vectors of the training set are known from the beginning and can be calculated if any of the labels are unknown, their operational data will be available to be used instead. Supervised learning is able to handle two main tasks, classification and regression.

Unsupervised learning does not require any label for the training set. It actually uses data that has no labels and the aim is to explore the data in order to find the objects that carry the same features, for example, distinguishing the customers with similar attributes who can then be treated similarly.

Unsupervised learning is typically used for clustering but there are many other problem examples like: given a video, specify a moving object and categorize in relation to other moving objects which have been seen [45] [47] [48].

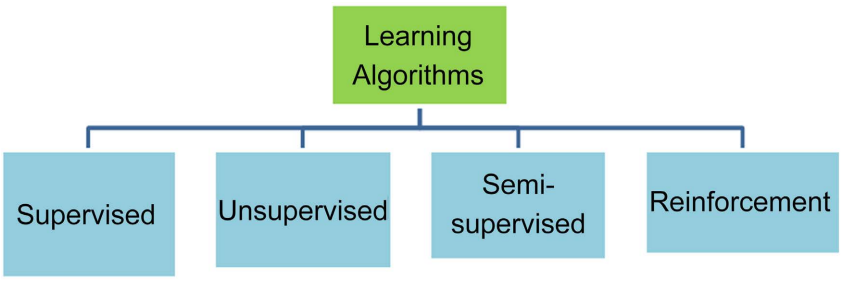

Figure 3. Types of learning.

Semi-supervised learning: is a combination of supervised and unsupervised learning. It works most of the time like the unsupervised learning, where the learning is essentially based on a set of unknown data which is generally deficient [45] [49].

Semi-supervised learning has been used in many domains such as video indexing, bioinformatics, and text processing. It can deal with classification, regression and prediction tasks [48].

Reinforcement learning is used to solve problems in which suitable action or sequence of actions should be taken. It works by keeping trying until it achieves the optimal goal, such as in driving vehicle, skill acquisition, game playing, robotics, and navigations.

In this learning type, the algorithms try to find the problem output according to set of parameters. Then, the predicted output becomes an input parameter and new output until the optimal output is achieved. Artificial Neural Networks (ANN) and Deep Learning, which will be presented in the following sections use this type of learning [37] [45] [47] [48] [49].

5.2.2. Review of Machine Learning Use in Various Fields

Machine learning has been used in a wide range of application areas, such as computer vision, face recognition, speech recognition, object classification, object detection, spam detection, fraud detection, advertising networks and bioinformatics [37]. The work in [35] presented an experimental study that combines support vector machine (SVM) with adaptive boost (Adaboost) for classification of pedestrian and vehicle image. The experiment is implemented on a large data set containing 4000 pedestrians. Many valuable results are obtained by analyzing the variances in performance caused by different training and test sets [35].

5.2.3. Machine Learning and IOT

ML algorithms have been involved in all the applications that based on data science such as data mining, information retrieval systems, search engines, big data analysis, text classification, object identification, and wide used in IOT applications [45] [50]. Many studies presented an overview of using IOT with ML in different applications and services and come out with the conclusion that machine learning gives devices connected to IOT a brain and make them able to think and make decisions [51].

Machine learning and its various techniques has been implemented in IOT security, such as in [52] which addresses the security issues regarding hardware, software, and protocol level in IOT platforms. Moreover, it provides a review of using machine learning approach for malware detection, behavior profiting, and fingerprinting [52]. Authors in [53] provide a valuable survey on the use of machine learning and deep learning methods for security of IOT systems. Their aim was to help researchers to effectively improving the security of IOT system [53].

In Internet of Vehicles (IOV), particularly in automobiles part, the major concern is traffic monitoring. So authors in [54] implemented ML approach that

uses data generated by cars to predict and identify traffic congestion [54].

5.3. Artificial Neural Network (ANN)

Artificial Neural Network (ANN) is inspired by the biological neural network of human brain, which is combination of large numbers of interconnected neurons, that are used to process input signals coming from various human body parts, such as: eyes, tongue, ears, nose, and hands.

Each neuron consists of three main parts:

1) Dendrite: is responsible of receiving input signals.

2) Soma: works as a processor, which collects and calculates the signals received through dendrite.

3) Axon: produce the output values that are calculated by soma.

ANN has a number of input with weights attached to each one of them, an activation function, and then the output will be obtained by applying the activation function to the weighted sum of inputs. Each part of the ANN is analogous to parts of biological neural networks, such as artificial neurons which has strong interconnection weight among units. The most important algorithms of artificial neural network are:

1) Perceptron.

2) Back-Propagation.

3) Hopfield Network.

4) Radial Basis Function Network (RBFN) [48] [55].

5.4. Deep Learning (DL)

The term Deep Learning is a powerful method that is considered a modern update of artificial neural networks. It is essentially concerned with constructing larger and complex neural networks with large number of hidden layers, that are suitable for handling big data such as data in image pattern recognition, speech recognition, and IOT applications. The most important deep learning algorithms are:

1) Deep Boltzmann Machine (DBM).

2) Deep Belief Networks (DBN).

3) Convolutional Neural Networks (CNN).

4) Deep Neural Networks (DNN).

5) Stacked Auto-Encoders [48] [49].

Review of Deep Learning Used in IOT Platform

Deep learning (DL) can allow IOT devices to interpret any data and intelligently react to both user and environmental events, but it has to regard performance and power requirement.

Some methods has presented the use of deep learning in IOT platforms such as the work in [55] has used deep learning (DL) technique to choose the useful information from huge volumes of multimedia data collected by IOT devices in smart agriculture environment that are utilized to improve the quality of life

(QoL) of farmers. However, they regard cloud computing in order to face the resource and energy constrains related to supporting deep learning in IOT devices. They also concerning with the delay on the network that caused by such kind of data [55].

Furthermore, Deep learning is widely used in IOT applications that are based on surveillance and object detection. Huge amount of data are need to be processed quickly and it requires quick response. In such case cloud computing is not useful because it is unable to meet the processing and response time requirements, so the problem can be solved using fog computing that has the ability to benefit the resources in the edge of the network along cloud resources. So the work in [56] has developed a deep learning-based fog cloud deployable system, called EdgeLens, for real object detection in IOT application platform. The proposed framework is deployed in fog cloud environment in order to leverage the advantages of fog computing to provide better quality for such IOT applications [56]. Also authors in [57] have presented an IOT discovery approach using Deep Neural Network (DNN) based on object detection. They apply You Only Look Once (YOLO) object detection algorithm to detect and localize signal objects in time and frequency [57]. Another method presented in [58] called IOT interaction, uses machine learning based gaze estimation and object detection technique to identify IOT devices, to allow the user to control the device by making specific hand gestures. The hand gesture, is recognized and sent as a command to IOT system to create the action [58].

Summary of the above reviewed method is shown in the following **Table 1**.

From the above review of machine learning, neural network and deep learning, we conclude that using such method will result in powerful and robust IOT object identity because it has the ability to perfectly deal with any classification problem and identification is considered a classification problem.

Table 1. Summary of the reviewed methods.

Article name	Citation	Investigator	Article synopsis
Deep Learning Entrusted to Fog Nodes (DLEFN) Based Smart Agriculture.	[55]	(applied Science) 2020.	Implementing deep learning technique for choosing the useful information from a huge volume of multimedia data gathered by IOT devices in smart agriculture environment.
EdgeLens: Deep learning based Object Detection in Integrated IOT, Fog and Cloud Computing Environments.	[56]	(ISCON) 2019.	A deep learning-based fog cloud called EdgeLens, has been developed for real object detection. It generally aims to provide better quality for such IOT applications.
Internet of Things (IOT) Discovery Using Deep Neural Networks.	[57]	IEEE (WACV) 2020.	An IOT discovery approach that uses Deep Neural Network (DNN) based on object detection.
A Smart Blind Interaction System Using Deep Learning.	[58]	(IJARCCE) 2020.	An IOT interaction model that aims to allow user control the IOT device by using hand gesture, which transmitted as a command to the IOT platform. The model uses machine learning base gaze estimation and object detection technique to identify the selected device.

6. Conclusions

The IOT concept is a new paradigm in which huge numbers of heterogeneous smart objects or things are connected to one Internet environment. IOT objects can interact with each other within the same environment and also with their neighbors. IOT aims to provide some services that benefit humanity and improve quality of their life.

The foremost important issue in all IOT platforms is to enable objects to be easily distinguished. This will be performed by identification, which defines proof of identity information for each object in the IOT world that usually identifies a unique object, such as a person, device, or any entity. The unique identity makes the object able to produce, process, and exchange data with other objects in the same or different scope. So the efficiency of IOT systems relies on the identification method applied to the system, which makes it necessary to adapt a robust identification method to ensure the best system performance. The problem of finding the suitable identification method for specific IOT platforms is however always a concern, that there is no common identification method that can be used for all IOT platforms yet.

The above literature of the existing object identification methods in IOT, shows that there are various identification methods used since the IOT concept was launched several years ago like: RFID, Barcode/2D code, IP address, EPC, etc. The rapid and continuous development in the field however requires development in identification methods as well, so there are many modern methods proposed recently based on various technologies such as computer vision, fingerprinting, machine learning, etc. Although there are many methods such as fuzzy logic, Neural Networks and Deep learning, can be adapted in many fields but have not been used for identification of IOT objects, and will lead to a significant change in the field if it is correctly used for that.

This paper provides an overview of the preceding identification methods as well as review of the modern identification methods on the various identity sectors, which were proposed recently by researchers and give details of some of the mathematical models they have proposed. By the end of this review we provide an introduction to fuzzy logic, Machine learning, Neural Networks and Deep learning, in addition to their uses for objects identification.

This review gives a deep understanding and enough knowledge about the various methods which exist and the value of using them for identification, which helps in deciding the use of Deep Neural Network for developing a new and robust identification technique for IOT objects.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Alpár, G., Batina, L., Batten, L., Moonsamy, V., Krasnova, A., Guellier, A. and Nat-

gunanathan, I. (2016) New Directions in IOT Privacy Using Attribute-Based Authentication. *Proceedings of the ACM International Conference on Computing Frontiers*, Como, 16-19 May 2016, 461-466. https://doi.org/10.1145/2903150.2911710

[2] Yadav, E. and Ankur, E. (2016) A Survey of Growth and Opportunity of Internet of Things (IOT) in Global Scenario. *International Journal of Innovative Research in Computer and Communication Engineering*, **4**, 20664-20671.

[3] Bernabe, J., Ramos, J. and Gomez, A. (2017) Holistic Privacy-Preserving Identity Management System for the Internet of Things. *Mobile Information Systems* (*MIS*), **2017**, Article ID: 6384186. https://doi.org/10.1155/2017/6384186

[4] Chibelushi, C., Eardley, A. and Arabo, A. (2013) Identity Management in the Internet of Things: The Role of MANETs for Healthcare Applications. *Computer Science and Information Technology* (*CSIT*), **1**, 73-81. https://doi.org/10.13189/csit.2013.010201

[5] Roman, R., Najera, P. and Lopez, J. (2011) Securing the Internet of Things. *IEEE Computer*, **44**, 51-58. https://doi.org/10.1109/MC.2011.291

[6] Hemalatha, D. and Afreen, B.E. (2015) Development in RFID (Radio Frequency Identification) Technology in Internet of Things (IOT). *International Journal of Advanced Research in Computer Engineering & Technology* (*IJARCET*), **4**.

[7] Bandyopadhyay, D. and Sen, J. (2011) Internet of Things—Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*, **58**, 49-69. https://doi.org/10.1007/s11277-011-0288-5

[8] Burhan, M., Rehman, R., Khan, B. and Kim, B. (2018) IOT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors*, **18**, 2796-2812. https://doi.org/10.3390/s18092796

[9] Marques, G., Garcia, N. and Pombo, N. (2017) A Survey on IOT: Architectures, Elements, Applications, QoS, Platforms and Security Concepts. In: *Advances in Mobile Cloud Computing and Big Data in the* 5*G Era*, Springer, Berlin, 2-24. https://doi.org/10.1007/978-3-319-45145-9_5

[10] Wani, U. (2019) An Introduction to IOT, Its Architecture and Various Protocols. IEEE Conference Paper, ID: 33482413.

[11] Ee, G., Ng, C., Noordin, N. and Ali, B. (2010) A Review of 6LoWPAN Routing Protocols. *Proceedings of the Asia-Pacific Advanced Network*, **30**, 71-81. https://doi.org/10.7125/APAN.30.11

[12] Polgavande, A. and Kulkarni, A. (2017) Internet of Things (IOT): A Literature Review. *International Journal of Research in Advent Technology*.

[13] Abdul, M.M. and Islam, N. (2012) Overview of Wireless Sensor Network. Intech, London. https://doi.org/10.5772/49376

[14] Gupta, C. and Kumar, A. (2013) Wireless Sensor Networks: A Review. *International Journal of Sensors, Wireless Communications and Control*, **3**, 25-36. https://doi.org/10.2174/22103279112029990001

[15] Ghumman, F. (2019) Effects of IPV4/IPv6 Transition Methods in IOT (Internet of Things): A Survey. https://doi.org/10.2139/ssrn.3402664

[16] Xiao, G., Guo, J., Xu, L. and Gong, Z. (2014) User Interoperability with Heterogeneous IOT Devices through Transformation. *IEEE Transactions on Industrial Informatics*, **10**, 1486-1496.

[17] Zarif, N., Najafi, H., Imani, M. and Moghadam, A. (2019) A New Hybrid Method of IPv6 Addressing in the Internet of Things. 2019 *Smart Grid Conference* (*SGC*), Te-

hran, 18-19 December 2019. https://doi.org/10.1109/SGC49328.2019.9056580

[18] Le, A., Loo, J., Lasebae, A., Aiash, M. and Luo, Y. (2012) 6LoWPAN: A Study on QoS Security Threats and Countermeasures Using Intrusion Detection System Approach. *International Journal of Communication Systems*, **25**, 1189-1212. https://doi.org/10.1002/dac.2356

[19] Jara, A., Varakl, S., Skarmeta, A. and Kirstein, P. (2014) Extending the Interne of Things to the Future Internet through IPv6 Support. *Mobile Information Systems*, **10**, 3-17. https://doi.org/10.1155/2014/831974

[20] Sanjeevi, V., Raj, K., Martin, J. and Rabara, S. (2018) An Integrated IPv6 Architecture for Smart Environment Using IOT and Cloud Computing. *Journal of Emerging Technologies and Innovative Research*, **5**, 69-72.

[21] Chalappuram, A., Sreesh, P.R. and George, J. (2016) Development of 6LoWPAN in Embedded Wireless System. *Procedia Technology*, **25**, 513-519. https://doi.org/10.1016/j.protcy.2016.08.139

[22] Gubbia, J., Buyyab, R., Marusic, S. and Palaniswami, M. (2013) Internet of Things (IOT): A Vision, Architectural Elements, and Future Directions. Elsevier, Amsterdam. https://doi.org/10.1016/j.future.2013.01.010

[23] Rimavicius, M. (2015) Literature Review of the Internet of Things: Anticipating Tomorrow's Challenges for Privacy and Security. Washington University, St. Louis.

[24] Kaur, K. and Kaur, K. (2017) Role of Rfid Technology in Internet of Things. *International Conference on Recent Trends in Engineering Science & Management*, Chandigarh, 8 January 2017, 166-174.

[25] Jia, X., Feng, Q., Fan, T. and Lei, Q. (2012) RFID Technology and Its Applications in Internet of Things (IOT). 2*nd International Conference on Consumer Electronics, Communications and Networks* (*CECNet*), Yichang, 21-23 April 2012, 1282-1285. https://doi.org/10.1109/CECNet.2012.6201508

[26] Byondi, F. and Chung, Y. (2019) Longest-Range UHF RFID Sensor Tag Antenna for IOT Applied for Metal and Non-Metal Objects. *Sensors*, **19**, 5460. https://doi.org/10.3390/s19245460

[27] Sackey, S., Kofie, S., Anajemba, J., Gapko, G. and Armah, A. (2019) A Concise Survey on Evolving IOT Security Technologies. *International Journal of Scientific Engineering and Science*, **3**, 42-47.

[28] Gil, D., Ferrández, A., Mora-Mora, H. and Peral, J. (2016) Internet of Things: A Review of Surveys Based on Context Aware Intelligent Services. *Sensors*, **16**, 1069. https://doi.org/10.3390/s16071069

[29] Orifama, D. and Okoro, H. (2020) Security Challenges in IOT Platforms and Possible Solutions. *Internet of Things and Cloud Computing*, **8**, 1-7.

[30] Aluthge, N. (2018) IOT Device Fingerprinting with Sequence-Based Features. Faculty of Science, Department of Computer Science, University of Helsinki, Helsinki.

[31] Rui, I., Toru, T. and Yuta, K. (2017) Individual Recognition Based on the Fingerprint of Things Expands the Applications of IOT. *NEC Technical Journal*, **11**, 1.

[32] Aneja, S., Aneja, N. and Islam, M. (2018) IoT Device Fingerprint Using Deep Learning. *IEEE International Conference on Internet of Things and Intelligence System*, Bali, 1-3 November 2018. https://doi.org/10.1109/IOTAIS.2018.8600824

[33] Bezawada, B., Bachani, M., Peterson, J., Shirazi, H., Ray, I. and Ray, I. (2018) IOTSense: Behavioral Fingerprinting of IOT Devices.

[34] Vaidya, G., Nambi, A., Prabhakar, T., Kumar, V. and Sudhakara, S. (2020) IOT-ID: A Novel Device-Specific Identifier Based on Unique Hardware Fingerprints. 2020

IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (*IoTDI*), Sydney, 21-24 April 2020. https://doi.org/10.1109/IoTDI49375.2020.00026

[35] Kaur, N. and Kaur, Y. (2014) Object Classification Techniques Using Machine Learning Model. *International Journal of Computer Trends and Technology*, **18**, 170-174. https://doi.org/10.14445/22312803/IJCTT-V18P140

[36] Sahni, S., Mittala, A., Kidwaia, F., Tiwaria, A. and Khandelwala, K. (2020) Insurance Fraud Identification Using Computer Vision and IOT: A Study of Field Fires. Elsevier, Amsterdam. https://doi.org/10.1016/j.procs.2020.06.008

[37] Malik, R., Kawoosa, A. and Zargar, O. (2018) Machine Learning in the Internet of Things—Standardizing IOT for Better Learning. *International Journal of Advance Research in Science and Engineering*, **7**, 1676-1683.

[38] Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N., Guarnizo, J. and Elovici, Y. (2017) Detection of Unauthorized IOT Devices Using Machine Learning Techniques.

[39] Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J., Ochoa, M., Tippenhauer, N. and Elovici, Y. (2017) ProfilIOT: A Machine Learning Approach for IOT Device Identification Based on Network Traffic Analysis. *Symposium on Applied Computing*, Marrakech, 3-7 April 2017, 506-509. https://doi.org/10.1145/3019612.3019878

[40] Hameed, K., Bajwa, I., Ramzan, S., Anwar, W. and Khan, A. (2020) An Intelligent IoT Based Healthcare System Using Fuzzy Neural Networks. *Scientific Programming*, **2020**, Article ID: 8836927. https://doi.org/10.1155/2020/8836927

[41] Sarwar, B., Bajwa, I., Ramzan, S. and Kausar, M. (2018) Design and Application of Fuzzy Logic Based Fire Monitoring and Warning Systems for Smart Buildings. *Symmetry*, **10**, 615. https://doi.org/10.3390/sym10110615

[42] Lloriana, D., Garcia, C., Bustelo, B., Lovelle, J. and Garcia-Fernandez, N. (2016) IoFClime: The Fuzzy Logic and the Internet of Things to Control Indoor Temperature Regarding the Outdoor Ambient Conditions. *Future Generation Computer Systems*, **76**, 275-284.

[43] Alshaer, J. (2015) Mobile Object-Tracking Approach Using a Combination of Fuzzy Logic and Neural Networks. *Global Journal of Computer Science and Technology: Network, Web & Security*, **15**, 19-26.

[44] Shukla, A. and Sahu, P. (2018) Design of Smart Home Security System Using Fuzzy Logic Based Internet of Things. *International Journal of Innovative Science, Engineering & Technology*, **5**, 154-169.

[45] Rana, A., Salau, A., Gupta, S. and Arora, S. (2018) A Survey of Machine Learning Methods for IoT and Their Future Applications. *Amity Journal of Computational Sciences*, **2**, 1-5.

[46] Ruta, M., Scioscia, F., Loseto, G., Pinto, A. and Sciascio, E. (2019) Machine Learning in the Internet of Things: A Semantic-Enhanced Approach. *Semantic Web Journal*, **10**, 183-204. https://doi.org/10.3233/SW-180314

[47] Mahdavinejad, M., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P. and Sheth, P. (2018) Machine Learning for Internet of Things Data Analysis: A Survey. *Digital Communication and Network*, **4**, 161-175. https://doi.org/10.1016/j.dcan.2017.10.002

[48] Dhage, S.N. and Raina, C. (2016) A Review on Machine Learning Techniques. *International Journal on Recent and Innovation Trends in Computing and Communication*, **4**, 395-399.

[49] Zantalis, F., Koulouras, G., Karabetsos, S. and Kandris, D. (2019) A Review of Ma-

chine Learning and IoT in Smart Transportation. *Future Internet*, **11**, 94. https://doi.org/10.3390/fi11040094

[50] Arora, J. (2020) IoT and Machine Learning—A Technological Combination for Smart Application. *International Conference on Innovative Advancement in Engineering and Technology*, Jaipur, 21-22 February 2020, 1-4. https://doi.org/10.2139/ssrn.3548431

[51] Swarnamugi, M., Chinnaiyan, R. and Ilango, V. (2016) IOT Technologies and Machine Learning Algorithms—A Study. *International Journal of Engineering Sciences & Research Technology*, **5**, 614-621.

[52] Mohaisen, A. and Kim, J. (2018) Securing the Internet of Things: A Machine Learning Approach.

[53] Al-Garadi, M., Mohamed, A., Al-Ali, A., Du, X. and Guizani, M. (2020) A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Communications Surveys & Tutorials*, **22**, 1646-1685. https://doi.org/10.1109/COMST.2020.2988293

[54] Kamble, S. and Kounte, M. (2020) Machine Learning Approach on Traffic Congestion Monitoring System in Internet of Vehicles. Elsevier, Amsterdam. https://doi.org/10.1016/j.procs.2020.04.241

[55] Lee, K., Silva, B. and Han, K. (2020) Deep Learning Entrusted to Fog Nodes (DLEFN) Based Smart Agriculture. *Applied Science*, **10**, 1544. https://doi.org/10.3390/app10041544

[56] Tuli, S., Basumatary, N. and Buyya, R. (2019) EdgeLens: Deep Learning Based Object Detection in Integrated IoT, Fog and Cloud Computing Environments. *International Conference on Information Systems and Computer Networks*, Mathura, 21-22 November 2019. https://doi.org/10.1109/ISCON47742.2019.9036216

[57] Lo, E. and Kohl, J. (2020) Internet of Things (IoT) Discovery Using Deep Neural Networks. *IEEE Winter Conference on Applications and Computer Vision* (*WACV*), Snowmass Village, 1-5 March 2020, 806-814. https://doi.org/10.1109/WACV45572.2020.9093371

[58] Logesh, N., Santhosh, S. and Subhashini, A. (2020) A Smart Blind Interaction System Using Deep Learning. *International Journal of Advanced Research in Computer and Communication Engineering* (*IJARCCE*), **9**, 49-52.