IoT-based Enterprise Resource Planning: Challenges, Open Issues, Applications, Architecture, and Future Research Directions

Article *in* Internet of Things · July 2020

DOI: 10.1016/j.iot.2020.100262

3 authors:

Madjid Tavana
La Salle University

Vahid Hajipour
Islamic Azad University West Tehran Branch

Shahrzad Oveisi
University of Tehran

IoT-based Enterprise Resource Planning: Challenges, Open Issues, Applications, Architecture, and Future Research Directions

Madjid Tavana[a,b,*]
[a]Business Systems and Analytics Department
Distinguished Chair of Business Analytics
La Salle University, Philadelphia, USA
E-mail: tavana@lasalle.edu
Web: http://tavana.us/

[b]Business Information Systems Department
Faculty of Business Administration and Economics
University of Paderborn, Paderborn, Germany

Vahid Hajipour[c,d]
[c]Department of Industrial Engineering
Islamic Azad University
West Tehran Branch, Tehran, Iran
E-mail: hajipour.v@wtiau.ac.ir

[d]Research Center, FANAP Co., Tehran, Iran

Shahrzad Oveisi[e]
[e]Research Center, FANAP Co., Tehran, Iran
E-mail: sh.oveisi@fanap.ir

DECLARATION OF INTEREST
None

ACKNOWLEDGMENT
The authors would like to thank the anonymous reviewers and the editor for their insightful comments and suggestions. Dr. Madjid Tavana is grateful for the partial support he received from the Czech Science Foundation (GAˇCR19-13946S) for this research, and Dr. Vahid Hajipour would like to acknowledge the support he received from the Research Center at FANAP Co.

*Corresponding author at: Business Systems and Analytics Department, Distinguished Chair of Business Analytics, La Salle University, Philadelphia, PA 19141, United States. Tel.: +1 215 951 1129.

IoT-based Enterprise Resource Planning: Challenges, Open Issues, Applications, Architecture, and Future Research Directions

Abstract

In today's highly competitive markets, organizations can create a competitive advantage through the successful implementation of Enterprise Resource Planning (ERP) systems. ERP works with different technologies, including the Internet of Things (IoT). IoT uses a unique Internet protocol to identify, control, and transfer data to individuals as well as databases. The data is collected through IoT, stored on the cloud, and extracted and managed in through ERP. In this study, we review the challenges, open issues, applications, and architecture of the IoT-based ERP. For this purpose, we review and analyze the latest IoT-related articles to present the unique features of the IoT and discuss its impact on ERP. The results show sensors and devices connected to the Internet can manage the stored data processed in the cloud through ERP without human intervention. We also discuss the challenges and opportunities in the relationship between ERP and the IoT risen by the introduction of the cloud.

***Keywords*:** Internet of things; enterprise resource planning; cloud computing.

1. Introduction

Companies in various industries collect different types of data, including invoices, customer information, project schedules, shipping, and payment information, among others (Rashid, 2002). Enterprise Resource Planning (ERP) plays a critical role in streamlining processes and improving business operations across industries (Mahmud, 2017). Today, the Internet of Things (IoT) and massive data influxes are stirring up the ERP landscape, introducing new possibilities for operational excellence and workflow automation (Snellman, 2017; Bahssas et al., 2015). IoT is evolving rapidly, and according to McKinsey's report on the global economic effect of IoT, the annual economic impact of IoT in 2025 will range from 2.7 to 6.2 trillion dollars (Andročec et al., 2018; Sha et al., 2019). However, in the midst of the excitement for increasing connectivity in manufacturing, the impact of IoT has on ERP systems, and business processes should not be overlooked (Balampanis et al., 2016).

Every system component in the IoT has an IP address, which enables the computers to identify, control, transfer data to other individuals, and related databases (Siddiqui et al., 2019; Siegemund and Turau, 2018). The collected data, stored in the cloud, enables ERP to manage, control, and process the data. Overall, the integration of ERP into IoT provides a great number of opportunities, the most important of which includes better management, automation, product traceability, and reduce ERP implementation costs (Zadeh et al., 2018). IoT creates a connection between the product and the customer by reducing human intervention and promoting automation using sensors. However, the integration of IoT into ERP faces a lot of challenges, and the biggest challenge is the lack of trust in IoT as a relatively new technology trend. Data security is a top concern, and companies heavily investing in ERP are very wary of the accuracy and reliability of the data coming from an IoT system (Sha et al., 2019; Stergiou et al., 2018). After almost three decades since their introduction, ERP systems are so well-oiled that a single record could represent a few million dollars. It is simply risky to trust new technology, and in a large-scale ERP implementation, nobody wants to save money unless it is millions of dollars (Snellman, 2017; Elmonem, 2016; Lenart, 2011).

In this study, we review the challenges, open issues, applications, and ERP-based IoT architectures. The latest journal papers at the intersection of ERP and IoT are reviewed and analyzed. We further demonstrate the relationship between ERP with cloud-based services. In Section 2, we present a brief history of ERP and IoT. In Section 3, we present the technologies and platforms in cloud ERP. In Section 4, we present the IoT, and in Section 5, we present our conclusions and future research directions:

2. History of ERP and IoT

Demonstrating a history of ERP systems, Table 1 shows that IoT was introduced in 1999 by Kevin Ashton (Alam et al., 2017). The growth of technology in ERP is also shown in Figure 1. As can be seen in Figure 1, the use of Internet technology in ERP has increased from 2000 with the use of the Internet and extranet technology (Sumner, 2014).

Insert Figure 1 and Table 1 Here

The evolution of ERP systems came just after the development of hardware and software systems. During the 1960s, most organizations designed, developed, and implemented centralized computing systems, most of which automated warehouse inventory control systems using inventory control (IC) packages. Essential Requirements Planning (ERP) systems were developed in the 1970s. In these systems, sectoral or product requirements planning is based on a comprehensive production plan. New software programs, such as product resource planning (MRP II), were introduced, focusing on the synchronization of the production process with the production requirements to optimize the production processes. Systems with ERP systems technologies first appeared in the late 1980s and early 1990s and had the power to coordinate and integrate operations throughout the company. Using MRP technology, ERP systems achieve the integration between business processes such as manufacturing, distribution, accounting, finance, human resources, project management, Inventory management, maintenance, and Logistics. This integration also creates accessibility and visibility, as well as unity throughout the company.

Developments in ERP include planning and scheduling (APS), Internet business solutions, including customer relationship management (CRM), and supply chain management (SCM). Figure 2 shows the major historical events related to ERP. During this decade, ERP has been associated with mainframe and mini and macro computer technologies, as well as data warehousing, data mining, knowledge management, and client-server networks with a distributed database and knowledge management. The first decade of the 20th century also saw ERP working with low-end IoT technologies, mainframes, client-server systems, distributed computing, Internet technology, and knowledge management. Today, there are many different systems on the market, most of which are migrating outside the cloud.

Insert Figure 2 Here

The company’s hardware provides the bases for the local installation of the conventional on-site ERP systems, while cloud ERP does not require such hardware. In other words, it is considered to be a service that works through providers and programs and is accessible through web applications. Each company can choose from a range of various ERP systems to deploy, and of course, the choice depends on a number of factors such as the data storage location as well as software hosting. The changes made to ERP implementation over time led to changes in the way the companies use ERP. Initially, the systems were small and not very functional, and they were developed to perform a specific task. So companies have no choice but to install and use various systems to perform all the tasks and provide management that a company needs. In many cases, the existence of small systems is indicative of the fact that there will be a lot of integration and communication among these systems. It also means that there is a lot of traffic coming through the network, and there are more risks involved, that is caused, ERP works with Internet technologies, mobile wireless, artificial intelligence, grid computing, knowledge management, web service architecture over the years and decades.As can be seen in Figure 1, the use of Internet technology in ERP has increased from 2000 with the use of the Internet and Extranet technology, which will reach its peak in 2020.

3. Cloud ERP: Technologies and platforms

This section will discuss cloud ERP technologies and platforms. First, the advantages and disadvantages of cloud ERP versus on-premise ERP are discussed in Table 2; then, different cloud ERP vendors are introduced, and ERP technology explored(Monk and Wagner, 2012; Rashid et al., 2002).

Insert Table 2 Here

As can be seen in Figure 1, distributed, web-based, artificial intelligence and other technologies have been more frequently used in recent years. Therefore, this report highlights five IoT technologies, namely blockchain, artificial intelligence, machine learning, and big data. The following will explore what platforms can work with these technologies. As shown in Figure 2, the platforms that can work with IoT include SAP, Oracle, Microsoft, Epicor, Sage, Netsuite, and People Soft.

The platforms that can work with blockchain technology include SAP, Oracle, Microsoft Azure, and IBM. SAP, Oracle, Microsoft Azure, and IBM are the technologies that can work with machine learning technology and artificial intelligence. Finally, the platforms capable of working with big data technology are SAP, Oracle, and Microsoft Azure (Snellman, 2017).

4. Internet of things (IoT)

The term Internet of Things (IoT) was coined by Kevin Ashton in 1999. He described a world where everything had a digital identity for itself and enabled computers to organize and manage things. For Kevin Ashton, “IoT” is a tool to overcome the domination of time and place. This view was first popularized by the Center for Automatic Identification and relevant market analysis publications(Mohammadi et al., 2018). RFID is considered as a prerequisite for this technology. From another perspective, the IoT is an environment where everything, whether human, animal or inanimate, possesses a unique Internet Protocol (IP) that has the ability to detect, control, send and transfer data to others and their respective databases. The data collected from objects will be visible through different tools such as mobile phones and a variety of computers and tablets. When IoT is implemented, data can be transferred across several objects. IoT is a function of the convergence and evolution of the three elements: Internet, wireless technology, and microelectromechanical systems. International Telecommunication Union defines IoT as follows: at any time and place, we will have something to which anyone can connect (Barcelo et al., 2016).

4.1. Integration ERP and IoT

Since the semantic web is considered to be an effective method for achieving the integration among systems, a model for integrating ERP and IoT is introduced here. Model of integration of cloud ERP APIs and things as a service (Darko Andročec et al., 2018). As shown in Figure 3, the IoT includes sensors, actuators, and applications (on mobile or Windows). Accordingly, the sensors collect data based on the actuator’s act. This information provides a common framework that allows data to be shared and connected to the cloud through the Semantic Web. The data is also linked to the IoT application via the cloud. ERP also manages and controls data through the cloud. The integration of IoT and ERP has many benefits, including the following:

1. Events such as re-orders, replenishment, out of stock inventories and missed deliveries could be informed automatically through sensors and devices connected to the internet.
2. IoT makes it possible to send notifications and warning to the manufacturers informing them that, for example, some of their products require their attention or some machines are down. Nevertheless, such a functionality is provided only when the business processes are adapted to this new model and be responsive to it.
3. IoT provides a considerable amount of data that needs to be gathered, processed, and analyzed

appropriately to gain the maximum benefits from IoT ERP. The robustness of this software program, however, is a genuine concern. IoT ERP is expected to deal with the massive influx of data from different devices and products. Thus, a lot of pre-preparation is demanded of the manufacturing companies while they need to take into account the size of their current ERP program and whether it is capable of connecting to IoT.

4. Real-time information is a prerequisite for an instant solution. The integration of ERP and IoT paves the way for real-time data and immediate solutions at the same time; this is possible through ERP, which provides a clear understanding of the situation while IoT offers the potential solutions. In fact, IoT will create junk information that can be extracted through ERP in an attempt to improve the business.
5. Through the sensors, this integrated system is able to protect company products from theft. It does this through an alert message such that if the package is manipulated before it gets to the destination, an alert message or an email is sent to the registered number or email address of the customer.
6. As for special or sensitive products whose maintenance demands special circumstances such as specific temperature or pressure, some IoT solutions safeguard these kinds of products against the environmental risks and keep the quality the same during the shipment.
7. According to the traditional methods, the manufacturer could only check on the quality of a product that has been shipped to the destination only through some primitive techniques such as customer service calls or field visits. However, the advent of technologies such as IoT makes it possible for the customer to trace the product's status and find out about its use, behavior, wear, and tear. Even some powerful IoT devices demand to replace their parts after they detect wear and tear.
8. There are two cases for selling the products: first, when the product is sold directly to the customer and second, when the product is sold through dealers. Of course, adopting the second approach poses a challenge to the ERP system in terms of keeping track of the end-users' data. However, by enabling the products to communicate with their customer immediately after they are initiated, IoT resolves this problem.
9. The automatic scan and entry of the barcode data are achieved through IoT in real-time. In other words, IoT reduces human intervention to a minimum through the sensors embedded inside the machines leading to improved production efficiency.

10. In a supply chain, IoT allows tracing the products or equipment as they are transferred from one stage to the next, and as a result, it provides real-time information. Subsequently, the real-time data is fed into the ERP system providing all those who are engaged with the supply chain with the feature which enables them to track the interdependencies between product life cycle and the material flow on the other hand.

Insert Figure 3

4.2. Analysis of published researches in IoT

As we have seen, IoT is one of the key technologies working with ERP. In analysis review sections, according to our investigation on the IoT field, 140 articles were randomly selected from recent IEEE, ACM, and Elsevier journals from IEEE Explore, ACM Digital library, Arvix repository, and Elsevier. By reviewing these papers, the journals in this field in our database are shown in Figure 4. As shown in this figure, a majority of articles in our database are derived from the IEEE database, IEEE Access, ACM database, ACM Transactions on Internet journal, and Future Generation Computer System from Elsevier database. The IoT review articles are shown in Table 3.

Insert Figure 4 and Table 3 Here

4.2.1. Taxonomy of IoT systems

After analyzing the papers, the following categories were identified based on applications, architectures, technologies, challenges, and topics to be discussed in the future, which are shown in Figure 5 and will be discussed in more detail below.

Insert Figure 5 Here

4.2.1.1. IoT system architecture

This section briefly describes the architecture of IoT systems. As can be seen in Figure 6, IoT networks include three layers, namely Application, Network, and Perception. Figure 6 shows the detailed architecture of IoT (Yang et al.,2011; Frustaci, 2017; Fang et al., 2014). The following example illustrates how IoT works. Smart parking, including sensors and microcontrollers, is located in each parking place. The user receives a live update about the availability of all parking places and chooses the best one. The ultrasonic sensors are used to relay information and display the available parking places in a web application. The IoT device consists of an ESP8266 microcontroller and an HC-SR04 distance measurement sensor. The sensor periodically measures the distance and transmits this data to the microcontroller, which is connected to AWS IoT service via the MQTT protocol. Periodically, the device sends measurements to the cloud where they are stored in AWS IoT shadow as a sensor state. A sensor detects a parked car by measuring the distance to the nearest obstacle. We used this example in parts a,b and c.

Insert Figure 6 Here

a) Physical layer

The physical object surface is involved with physical IoT sensors. The physical object is mainly involved with sensing, collecting, and sometimes processing information. At this level, diverse sensing functionalities are implemented through adapting sensors and actuators such as temperature, motion, or acceleration sensors. In the smart parking example, the ultrasonic sensors are in the physical layer.

b) Connectivity

One of the main goals of the IoT platform, communicate Heterogeneous sensors cooperatively, and subsequently provide smart services. Since the sensors deployed in IoT use battery for their power and their computation as well as storage capacity are limited, they are considered resource-limited. Therefore, IoT sensors should work with low-power sources under a lossy and noisy communication environment. Recent IoT communication technologies: 6LoWPAN, Bluetooth, IEEE 802.15.4, WiFi, ultra-wide bandwidth, RFID, and near-field communication. In the smart parking example, the AWS IoT core is the service that manages the connection with the cloud.

c) Middleware

Middleware aims at demonstrating the complexity of a hardware system, and of course, this means more concentration on the problems by the developers without being disturbed at the hardware level. Several interfaces can be used to connect us to sensors and other objects, including Bluetooth, WI-Fi, RFID, and NFC. In a smart parking example, the AWS IoT Platform is middleware.

d) Hardware-level

Hardware complications are usually caused by related to communication and computation issues. A software level is provided across operating systems, applications as well as the network communication levels by the middleware, enabling cooperative processing. From a computational standpoint, a middleware provides a level that sits between application and system software and has the following main functions. First, it allows for collaboration between heterogeneous IoT objects so that diverse IoT classes communicate with each other without interruptions through the middleware. Actually, the middleware plays a significant role in enabling the interoperability among IoT devices. The second major role played by the middleware concerns the devices, which are potential for interaction within the IoT domain. In fact, it provides these devices with scalability.

The evolution of IoT devices is expected to be the outcome of middleware through critical reforms being made when scaling up the organization. The third role is the device discovery and environmental awareness, which has to be provided by middleware to support object knowledge of other surrounding IoT objects. Middleware is also in charge of providing the type of computing that is environmentally conscious so that the sensors' data become understandable, which can be employed to provide context and present intelligent services to users. Finally, in another role, the middleware addresses IoT security as well as its privacy, and that is because of human or industry involvement with the data presented by IoT. In other words, it is essential to take into account the sensitive issues of security and privacy; moreover, the firmware is expected to consider mechanisms to create a secure IoT system (Al-Garadi et al., 2018; Saheb and Izadi, 2019).

e. Big data analytics

The noticeable amount of data captured by IoT is highly valuable. Several physical objects existing in the different IoT applications are in charge of creating such big data. Thus, the large amount of data generated by the physical devices must be analyzed online to acquire useful knowledge. The timing of knowledge acquiring is useful. According to researchers, there are various ways to integrate big data analytics with IoT design so that this data becomes understandable. ML and DL go beyond the traditional analytic methods; in fact, they are capable of absorbing the invisible insight of big data and transforming it into useful data with a minimal human contribution (Al-Garadi et al., 2018).

4.2.1.2. Applications of IoT in ERP systems

IoT has several applications. The analysis of articles available in our database identified the applications of IoT shown in Figure7 and Table 4 along with the articles in our database (Smart grid, health care, monitoring, smart home, security, wearable devices, smart city, and energy). The most common applications of IoT were in Smart City (road management, smart agriculture, smart transportation, smart parking, and smart university), health care, and security.

Insert Figure 7 and Table 4 Here

a) **Smart city**

Cities inherently face complex, widespread, and interconnected challenges that can only be solved using a systematic approach. In other words, the massive crowding of residents leads to chaos, creating conditions that not only bring down the equilibrium of cities but prevent sustainability with current methods of urban management and development. Therefore, urban planners all over the world try to develop models of 21st-century urban development, satisfying the new demands and expectations of today's world with an integrated view for all aspects of urbanization. The development of a smart city is a new concept to address the current challenges of cities in the field of urban planning, which has attracted a lot of attention in recent years. A smart city has been the focus of the millennium transformation and development, which means opening new concepts in urban planning that combine the capabilities of real and virtual worlds to solve urban problems (Marjani et al., 2017).

The ERP systems govern rules for purchasing, inventory usage, permitting, and billing. The city finance department tracks all public expenditures and incoming payments via the ERP system. Public works and city engineering utilize the work order system within the ERP system to respond to city building issues or infrastructure issues reported by citizens or identified by the real-time event management and analytics system.

Planning, permitting, and inspections use geographical information systems (GIS) to manage the planning process for land usage throughout the city. The permitting process utilized with the ERP system allows permits to be requested online, and then the citizen or business can track the permit and inspection process as it is completed.Permits are issued online via the ERP permitting web portal. The permit process includes inspections of retention ponds throughout the city. The sensor network IoT will be utilized to provide water quality information and foliage growth data (Siegemund and Turau, 2018).

b) **Smart health care**

The IoT devices have become the heart of key health applications recently, having received a boost from the healthcare sector. Monitoring the health status of the patients, recording their information, notifying the related healthcare system of the critical circumstances, and subsequently facilitating the process of treatment for the patient in a timely manner is, among others, the significant roles of IoT devices in the healthcare systems. With almost 60% of the healthcare sector has implemented the Internet of medical things (IoMT) devices, the IoMT is believed to be leading to a revolution in the domain by turning disorganized healthcare into a synchronized one. IoT devices made almost 30.3% of 4.5 billion IoT devices in 2015; however, the statistic had been predicted to rise to 20-30 billion by 2020 (Afzal et al., 2017; Marjani et al., 2017; Baker et al., 2017).

ERP, on the other hand, plays a major role in the healthcare sector by achieving an effective integration among the processes and the services.ERP would make a big difference in areas such as finance, human resources, and revenue and admission resources of the healthcare sector if it were implemented successfully. Services such as diagnosis, patient's home care, and chronic care are provided by the healthcare system through the information they receive from various sources. Needless to say, these various sources and processes will be much more helpful for the healthcare system if they are integrated because integration allows for more information sharing while the traditional models are based on segregated processes and thus less information sharing. So by achieving integration across various systems in different locations and having access to them, ERP smoothes the healthcare processes, improve the quality of their services, and help the health fraternity to be more efficient in their jobs. Implementing ERP in a hospital is particularly beneficial for the front desk as well as the financial management sections.ERP provides the front-desk staff with the information they require, such as appointment, bed availability, specialized services, and the doctors' schedules leading to the organized and effective performance of the front desk. The financial management also benefits from ERP because it offers solutions to cut costs, produce more comprehensive managerial reports, and reduce risks.

c) **Smart monitoring**

IoT monitoring has many advantages, some of which are listed below:

- It helps in analyzing the dynamic systems and processing a large number of events and alerts.
- It also gathers and analyzes IoT data from connected devices and applications and thus create integration between the devices and business.
- It optimizes the performance across multiple applications, APIs, networks, and protocols and thus bridges the performance gaps
- It provides you with feasible insights to create a better customer experience, mitigate the problems, and increase the IoT opportunities.

d) **Smart home**

Human presence detection, activity detection, self-organizing appliances, air conditioning control based on user desire and convenience, etc. are made possible by machine learning. In particular, the detection of activity due to its use in life support, home automation, etc., has received much attention (Samie et al., 2019). For example, information regarding energy status, including its availability and price now or in the future, is provided by energy sources such as photovoltaic appliances and power suppliers. This information is used by devices which are considered the subscriber in an attempt to modify their patterns.

e) **Smart grid and smart meter**

Smart grid deals with effective ways to effectively manage and control energy production costs and save energy, which proves to be more reliable in achieving these goals than the conventional grid. Moreover, smart meters as modern energy meter makes power consumption measurable and help to monitor and control electrical devices.

The smart grid, which is a flexible system connecting people with technology and natural systems, can be defined from functional or technological perspectives. It includes an electric grid, a communications network, and controlling and monitoring hardware and software and is capable of providing power, reducing costs, and presenting instant information. For example, the digital electricity grid which gathers and pass information, and creates electricity using the bilateral technical direction (Marjani et al., 2017).

In relation to the smart grid and the onslaught of big data, financial transformation is achieved as a result of the demands of business transformation. Since utility companies are encouraging industry-changing advancements of this type, ERP systems strive to offer strategic insights for the better management and application of the gathered data.

4.2.1.3. Relation with other technologies

Another issue discussed in papers is the relationship of IoT with other technologies. As can be seen in Figure 8, machine learning and deep learning technologies make the most use of and have synergy with IoT technology in reviewed papers. To this end, we also examined a variety of methods used in this field among the articles, the results of which are shown in Figure 8.

Insert Figure 8 Here

a) Machine learning and deep learning methods in IoT

Recently, a lot of IoT-based applications have emerged in various vertical fields, namely health, transportation, smart home, smart city, agriculture, education and so forth most of which are based on intelligent learning mechanism for prediction (i.e., regression, classification, and clustering), data mining, and pattern recognition of data analysis in general. Recently, deep learning (DP) has been employed in IoT applications more than other machine learning approaches. According to an announcement made at the Gartner/ITxpo 2016 Symposium, DL and IoTwere among the top three strategic technology trends in 2017. This widespread advertising for DL points out the fact that the traditional machine learning approaches do not meet the newly identified analytical needs in the field of IoT. In other words, according to the hierarchy of IoT data generation and management, various modern analytical and artificial intelligence (AI) approaches are what IoT systems demand. The growing interest in IoT and the big data, which have a reciprocal relationship, demands shareholders who clearly understand its definition, components, potentials, and challenges. On the one hand, IoT is the major generator of big data, and on the other hand, IoT services are an essential target for analyzing big data to improve processes. In addition, big IoT data analysis has proven to be valuable to the community. For example, it was reported that identifying the damage to pipes and fixing them saved nearly one millionUS$ in the water bills of Miami Park Administration (Al-Garadi et al., 2018). DL models generally bring about two important advances relative to traditional machine learning approaches in training and prediction stages. Firstly, they reduce the need for manual, human-made, and engineered feature sets for use in education. As a result, some features that may not be apparent for men are easily extractable by DL models. Moreover, DL models improve accuracy. Neural networks and deep learning methods are generally used in ERP-based IoT systems for the following cases:

- **Advanced analytics**

Machine learning and deep learning methods allow for handling a large amount of data paving the way for real-time and accurate data insights. As an example, we refer to AI for analyzing different types of customers' buying behavior, providing one with the opportunity to adapt products or services to the needs of a specific audience.

- **Warehouse management**

There are a large number of demand forecasting models which can be tested accurately using machine learning and deep learning methods to adapt various kinds of variables such as change in demand, supply chain disruptions as well as new product introduction.BMW, for example, traces an item from the time it is being manufactured until the moment it's sold using learning algorithms while monitoring 31 assembly lines in different countries.

- **Forecasting**

Machine learning and deep learning methods help find solutions that are capable of processing historical data and predicting the future. In the business world, these methods help identify seasonal patterns and provide suggestions regarding the production volume.These forecasting methods provide the business world with more accurate predictions in a more cost-effective way and thus help avoid overproduction or underproduction by guiding through the decisions regarding the manufacturing volume.

- **Financial management**

Machine learning and deep learning methods allow the automation of quarterly and monthly processes and the closure of operations after the accuracy reports are verified, and the account balances are compared. Invoice data can be categorized into different accounts using these methods, enabling us to differentiate between a phone purchase and a monthly phone bill.

- **Interdepartmental processes**

It is complicated to integrate sales, inventory, and accounting. However, Artificial Intelligence is not afraid of massive amounts and various types of data, making it the perfect solution for creating a centralized platform.

- **Customer service**

In the case of field services, these methods provide users with the information regarding performance evaluations and the qualification of the employees so that the planning is facilitated and the service calls are scheduled.

- **Production processes**

In case of integration with ERP these methods, help to identify the inefficient processes and offer a solution to reduce costs. Moreover, these methods help to detect energy-consuming processes and facilitate predictive diagnoses and thus contribute to less waste of resources.

- **Human resources**

ERP software enabled by AI can be proactive, and this is a big advantage because, for example, it can analyze the applicants' data based on their qualification parameters such as skills and experience, it can find out which employee needs to be promoted.

- **Sales automation**

Chatbots powered by AI help not only customers but also conduct the whole sales triangle. Now, bots can cope with segmentation and provide responses in real-time. After reviewing our database, the methods used in these articles are as follows (shown in Figure 9). Accordingly, SVM, CNN, reinforcement learning, and autoencoder were the most commonly used tools in the articles. Some of these articles are discussed below;

Insert Figure 9 Here

Another framework operating within the IoT ecosystem was presented by Khelifi et al. (2018) for a decision-support system (DSS). The proposed framework, which has been compared with three machine learning prediction model classifiers, i.e., Naïve Bayes, Random Forest, and Decision Tree and empirically evaluated using data sets from a commercial network, demonstrated efficiency with a complete Bayesian network prediction model. Chen and Hao (2019) concentrated on feature dimension reduction of wireless communication signals and took the power amplifier radio frequency (RF) fingerprinting as an example of the output of their efforts. The researches conducted on the RF fingerprint feature dimension reduction method focus mainly on reducing the high dimensionality of RF fingerprint features and the uncorrelated or redundant features in the features space. In another paper, Tang et al. (2017)describe how CNN inference engines can enable deep-learning tasks on IoT devices. Ateeq et al. (2019) employed historical data from machine learning (ML) and proposed a proactive architecture for prediction. Their proposed model named adaptive moving window regression (AMWR) was derived from an adaptive prediction algorithm and was evaluated using a real-world use case (traffic data provided by the city of Madrid) with an accuracy of over 96%. Adnan Akbar et al. (2017) presented a proactive architecture that exploits historical data using machine learning (ML) for prediction in conjunction with complex event processing. A semi-supervised deep reinforcement learning model was introduced by Mohammadi et al. (2018), which employs Variational Autoencoders (VAE) as the inference engine to generalize optimal policies. This model can be deployed in applications related to smart cities using labeled and unlabeled data to facilitate the performance as well as the accuracy of the learning agent.

Tekeste et al. (2018) concentrated on developing technologies such as Machin Learning (ML), cloud Computing as well as IoT in an attempt to develop a more cost-effective system for water quality monitoring replacing the traditional way of quality monitoring. Xiao et al. (2018), on the other hand, concentrated on the IoT system from different perspectives such as the attack model, security solutions based on different techniques of machine learning such as supervised learning, unsupervised learning, and reinforcement learning. Samie et al. (2018), Mohammadi (2018), Khelifi (2018), and Al-Garadi et al. (2018) presented infrastructure toolsets that provide elastic provisioning of application components on resource-constrained and heterogeneous edge devices in large-scale IoT deployments. After reviewing the papers and results, we have discussed the machine learning and deep learning approaches in more detail. The advantages, disadvantages, and applications and references to these methods are presented in Tables 5 and 6.

Insert Tables 5 and 6 Here

4.1.3. The challenge related to cloud ERR and IoT

Several challenges have been discussed in the reviewed articles. As mentioned, because IoT systems are associated with cloud ERP, many challenges, open issues, and future directions are associated with cloud services (Brous et al., 2019; Karimanzira and Rauschenbach, 2019; Gubbi et al., 2013; Amendola et al., 2014; Kamilaris and Pitsillides, 2016; Cai et al., 2017; Samie et al., 2018; Cui et al., 2018).

1.1.3.1.Heterogeneity

A big problem with the cloud ERP-IoT paradigm lies in the extensive heterogeneity of available devices, operating systems, platforms and services, and possibly recently upgraded applications. cloud platform heterogeneity is not something to be overlooked. Typically, there is an overlap in ownership of objects for cloud services, allowing for proper merging and customization of resources according to each provider. This problem is exacerbated when users take advantage of multiple cloud platforms.

Providers should consider target scenarios, analytic requirements, choice of hardware and software environments, a combination of heterogeneous subsystems, development, and delivery of computing infrastructure, and provision of maintenance services for each service or application. On the other hand, thanks to the presentation paradigms of cloud services, it is hoped that the IoT paradigm will easily end up in IoT service provision, although the implementation requires solving the big problem of heterogeneity. For example, it is necessary to appropriately combine (and manage) a large number of highly heterogeneous objects (and their correspondingly generated data) across different levels of the cloud platform. This problem encompasses a variety of dimensions, and its solutions are under consideration based on integrated platforms and middleware, interactive programming interfaces, duplication tools in the presence of data variety, and so forth (Alam et al., 2017).

4.1.3.2. Functionality

In this section, we focus on the challenges related to Functionality discussed in the reviewed articles:

a) Performance

Most cases of cloud ERP-IoT paradigm applications provide specific functionality and quality of service (QoS) requirements (for example, communication and computing and storage aspects) and, in some scenarios, meet requirements that are not easily accessible. Specifically, achieving stable and acceptable network performance for the cloud paradigm is a major problem as the increasing bandwidth does not lead to an evolution in storage and computing since timeliness is greatly influenced by unpredictable problems, real-time applications are essentially vulnerable to performance bottlenecks.

b) Latency (Delay)

The term latency, also known as turnaround time, in the context of mobile cloud computing, means the time when the computation is offloaded, and the results are received from the nearby infrastructure or cloud.

c) Energy efficiency

Energy efficiency refers to a way through which the growth of energy consumption can be managed and prevented. By delivering more services for the same energy input or for the same services for less energy input, maybe something more energy efficient.

d) Resource limitations

Since the IoT architecture is resource-constrained, it has been difficult to define a robust security mechanism for it, and thus in order to work within such constraints, the algorithms have to be limited. For a successful implementation of IoT security and communication protocols, the storage and energy requirements need to be managed with each broadcast or multicast necessary for keys or certificates exchange. This means that these protocols should be lightweight and energy-efficient despite the complicated computations and improved energy harvesting techniques.

e) Cost-effectiveness

A major challenge for the SIoT application is to provide an efficient and profitable service development for energy and computing costs. A major challenge for the SIoT application is to provide an efficient and profitable service development for energy and computing costs. Multiple processes can run simultaneously, which may change as per variation in applications and user requirements.

f) Reliability

In the field of intelligent transportation, cars are usually on the move most of the time, and vehicle networking and communications are often disrupted or unreliable. When using applications in limited-resource environments, there are a few problems with a crash or lack of sustained availability of the device. On the other hand, cloud capabilities help overcome some of these problems; for instance, cloud technology improves the reliability of devices by making it possible to reduce the burden of heavy tasks and thereby increase battery life or enable modular architecture; alternatively, the technology itself has uncertainties regarding data center virtualization or resource depletion.

4.1.3.2. Large scale

New applications can be designed using the cloud ERP-IoT paradigm to integrate and analyze the information received from (embedded) real-world tools. Some of the presented scenarios implicitly require interaction with a large number of these tools, which are usually scattered across large environments. The large scale of the mentioned systems makes it more difficult to solve common problems (for example, when dealing with long-life data that are collected at high speeds, the requirements of storage capacity and computing capability will be increasingly difficult to meet). In addition, the distribution of IoT tools complicates monitoring tasks due to dynamic time lag and connectivity issues.

4.1.3.3. Big data

Special attention must be paid to the transfer, storage, and access and processing of the enormous amount of data that will be generated given 50 billion devices estimated to be connected to the network by 2020. Thanks to recent advances in technology, IoT will be a major source of big data, and our cloud system enables us to store and analyze complex data for long periods and perform complex analytics on them. The ubiquity of mobile devices and sensors inevitably requires scalable computing platforms. Convenient handling of this volume of data is a sensitive issue since the overall performance of applications depends heavily on the features of data management services. For instance, cloud-based approaches to summarizing big data based on extracting semantic features are under investigation. Hence, following the NoSQL movement, both proprietary and open-source solutions use alternative database technologies for big data, which includes: time series, key-value, key-value repositories, large column repositories, and graph databases. Unfortunately, there is no excellent data management solution for the cloud system to handle big data. Moreover, data integrity is considered an important factor not only because of its impact on service quality but due to the security and privacy dimensions that are particularly relevant to outsourced data.

4.1.3.4. Sensor network

Sensor networks have been defined as the major enablers of IoT and one of the five technologies that are shaping our world, giving us the ability to measure, understand and perceive environmental signals; recent advances in technology have allowed for efficient, inexpensive, and low-cost small tools to be used for remote sensing applications on a large scale. Furthermore, despite their limitations in battery consumption and reliability, smartphones have multiple sensors (GPS, accelerator, digital compass, microphone, and camera) that support a wide range of mobile applications in various areas of IoT. In this context, the timely processing of massively transmitted sensor data, which are vulnerable to power and network constraints, is a newly introduced problem. The cloud system offers new opportunities to collect sensor data and use them for widespread coverage and relevance, but at the same time overshadows the privacy and security aspects. In addition, although IoT devices are not mobile, which is considered a common dimension, the sensitivity of sensors in smartphones and wearable electronics devices is still a problem.

4.1.3.5. Monitoring

It has been widely documented in resources that surveillance is an essential activity in cloud environments for capacity planning, resource management, service level agreements, performance, and security as well as troubleshooting. As a result, the cloud ERP-IoT paradigm has the same regulatory requirements as the cloud system; however, the problems associated with this paradigm are also sensitive to the properties of the volume, variety, and speed of IoT.

4.1.3.6. Fog computing

Fog computing is part of the classic cloud computing operating on the periphery of the network. It is a system designed to support IoT applications with features such as time delay constraints and requirements concerning mobility and geographic distribution. Although computing, storage, and networking of resources are both cloud and fog systems, the latter has certain features as follows: being on the edge of the network and aware of the time-delayed geographic location; geographic distribution and a large number of nodes compared to concentrated cloud system; support for object mobility (via wireless communication) and real-time interaction (rather than batch processing); support for interaction. It is difficult to design cloud computing projects in multiple forms. Certainly, adopting cloud-based approaches requires a variety of specific algorithms and methodologies that examine the reliability of smart device networks and operate under specific conditions demanding error-resolving methods.

4.1.3.7. Security

This section discusses the security challenges discussed in the articles (Restuccia et al., 2018).

- **Security and trust management**

When it comes to the widespread adaptation of technology, security is always a critical issue. It is essential to establish a trust to strengthen communication among two or more IoT devices. Efficient authentication and trust management tasks in different SIoT application scenarios need to be ensured through flexible and strong security protocols within OS, each of which may require a specific kind of encryption algorithm. However, for implementing these algorithms, they need to be computationally less intensive; they need to operate in real-time to prevent performance degradation, and finally, they should take into account the memory and latency requirements. Correspondingly, the memory handling can also raise security concerns.

- **Privacy**

Data privacy is of great significance since it poses a major challenge preventing consumers from adopting cloud computing. The consumers' trust must be established to meet this challenge, and this can be achieved when the application models cover application development with privacy protection and implicit authentication mechanisms (Marjani et al., 2017).

4.1.3.8. Complex environment

A complicated IoT ecosystem is made of various elements such as software programs, hardware devices, different connected objects, and, most importantly, a large number of end-users. Some practical applications are built based on this ecosystem, demonstrating its influence. However, real-time IoT applications mostly demand a large amount of data, which requires storage and processing resources to extract intelligent information, and this is almost an uncharted territory in the existing IoT literature.

4.1.3.9. Real-time processing

Since a considerable number of requests from various types of smart applications along with fast responses are managed in the IoT ecosystem simultaneously, compared with the cloud-based applications, IoT applications impose multiple requirements regarding the resources for real-time and online processing. This turns the spotlight on the resource management of such a complicated ecosystem and highlights the critical issue of multiple orders which demands brand new solutions.

4.1.4. Open issues and future direction

This section discusses open issues and future direction. As mentioned, many issues are related to these three areas due to ERP's relationship with cloud and IoT services (Samie et al., 2019).

4.1.4.1.Open issues

This section focuses on the open issues discussed in the articles:

a) Standardization

The lack of standards has been considered by many researchers as a major issue in cloud IoT. Most objects are now connected to the cloud via web-based interfaces, which have the potential to reduce complexity in the development of such applications. Similarly, both clouds and objects are implemented using non-standard heterogeneous interfaces. Although the scientific community has contributed to the deployment and standardization of IoT and cloud phenomena, the need for standard protocols, architectures, and API software interfaces is evident to facilitate the interconnection between heterogeneous smart objects and the creation of advanced services realizing the phenomenon of cloud IoT.

b) Big data

cloud IoT involves managing and processing large amounts of data and events from different situations and heterogeneous source types so that most applications require complex real-time operations. On the other hand, this means proper synchronization of events from remote sources, reconstructing and correlating their semantics for meaningful deduction of the status of a particular application. Alternatively, this signifies processing a lot of multimedia data in real-time for the timely extraction of the information needed to set up affiliate services and assist the user in their current state.

c) Security and privacy

Security and privacy are considered both as a research challenge attracting a lot of attention and an open issue that still needs further work. Although many users are now worried about privacy and security in cloud-based applications, such concerns are all the more important as cloudIoTimports real-world data into the cloud and trigger real-world actions. With respect to privacy, providing the right roles with appropriate design and security is still a challenge, while clearly ensuring that only authorized people have access to sensitive data, especially when data integrity must be guaranteed in response to permitted changes.

With regard to security, it remains challenging to deal with various hacker threats since malicious software can be injected into physical sensors to provide manipulated data; raw or processed data can be stolen or tampered with on cloud; compromised gateways can violate cloud IoT system security; communication channels are vulnerable to leakage of side-channel information.

d) Intelligence

Focusing on real-time data coming from inhomogeneous objects enhances increased decision-making abilities using information combination and selection mechanisms. Although there have been researching efforts in this area, maximizing intelligence in this field is still an obvious challenge.

e) Integration methodology

As long as cloud IoT solutions are built around specific applications, little effort has been devoted to developing a common methodology for the integration of cloud systems and IoT. Because the suite of applications has defined requirements, standard multi-tasking can be described. Moreover, a flexible, public platform can be a starting point for easier implementation of such tasks.

f) Network communications

cloud IoT includes several heterogeneous network technologies where many applications require continuous data transfer, and overall bandwidth consumption is dramatically increased. On the one hand, the efficiency of access management for enabling continuity and optimizing bandwidth utilization is still an open issue. Alternatively, the current bandwidth constraint cannot support this increasing trend, and further research work is needed to refine large-scale allocation methods.

g) Storage

Storage solutions have been discussed in several articles. For instance, we have already considered them as an outcome for the integration of cloud and IoT. Nevertheless, articles continue to address this issue as an open one because current solutions may not provide the support needed for future applications. While data must receive time labels to enable server-side reconstruction and processing, the transfers need proper scheduling to avoid over-networking and load processing. A likely orientation to address such a topic involves the introduction of prophetic storage and concealment.

5. Conclusions and future research directions:

The organizations' awareness of the changes in ERP plays a significant role in customer satisfaction. Intelligent devices that provide organizations with online data about their product, their quality, their transportation, etc. can have a drastic influence on not only the customer services but also on better management of the whole organization. However, cloud ERP integrated with IoT is a modern area promising more fulfilling management as well as customer services.

In this article, because of the impact of IoT on cloud ERP quality, our primary focus was on identifying important IoT features by analyzing articles from recent scholarly and academic journals. We presented a history of ERP and IoT, along with cloud ERP and IoT technologies and platforms. We further discussed the integrated ERP and IoT and analyzed recently published research in IoT. We presented a taxonomy of IoT systems and architecture with applications of IoT in ERP systems. Finally, we presented the challenge related to cloud ERR and IoT and presented future research directions in the integrated ERP and IoT research.

Further research efforts are expected in several directions to realize the full potential of the cloud IoT (Samie et al., 2019; Gubbi et al., 2013; Frustaci, 2017):

- Proper identification, naming, and addressing of objects to support a large number of objects as well as real-time mobility. While IPv6 may be a viable solution, large scale adoption of it, is still an ongoing process. Further research is needed in specific scenarios to accelerate this slow process (such as access networks) and in dealing with new drivers and scalable requirements.
- Solutions for detecting environmental changes based on IoT data will enable the delivery of advanced content-based services. Such an opportunity leads to research on more effective ways to deliver personalized content and advertising.
- Large-scale support is necessary for multi-network scalers (such as multi-homing, multi-path, multi-cost), connection delivery, and roaming to improve network reliability and ensure continuous connectivity, QoS, redundancy, and error tolerance. Software-based network solutions are also expected.
- Many cloud-based IoT applications can utilize efficient and flexible mechanisms to create logical discrete network partitions without the need for globally distributed network infrastructures, which could be another important driver for research into network virtualization and software-centric networks.
- Convergence towards a common open-service infrastructure environment provides APLs with the third-party deployment of cloud-based applications. This convergence will provide new business opportunities and result in research efforts to define standard protocols, libraries, languages , and methodologies for the cloud computing Internet.

References

Accenture Enterprise Services for Utilities, Delivering high performance in enterprise resource planning, 2013.

Afzal, B., Umair, M., Shah, G. A., & Ahmed, E. (2019). *Enabling IoT platforms for social IoT applications: vision, feature mapping, and challenges*. Future Generation Computer Systems, 92, 718-731.

Akbar, A., Khan, A., Carrez, F., & Moessner, K. (2017). *Predictive analytics for complex IoT data streams*. IEEE Internet of Things Journal, *4*(5), 1571-1582.

Alahakoon, D., & Yu, X. (2015). *Smart electricity meter data intelligence for future energy systems: A survey.* IEEE Transactions on Industrial Informatics, 12(1), 425-436.

Alam, F., Mehmood, R., Katib, I., & Albeshri, A. (2016). *Analysis of eight data mining algorithms for smarter Internet of Things (IoT).* Procedia Computer Science, 98, 437-442.

Alam, F., Mehmood, R., Katib, I., Albogami, N. N., & Albeshri, A. (2017). *Data fusion and IoT for smart ubiquitous environments: a survey. IEEE Access*, 5, 9533-9554.

Al-Garadi, M. A., Mohamed, A., Al-Ali, A., Du, X., & Guizani, M. (2018). *A survey of machine and deep learning methods for internet of things (IoT) security*. arXiv preprint arXiv:1807.11023.

Amendola, S., Lodato, R., Manzari, S., Occhiuzzi, C., & Marrocco, G. (2014). *RFID technology for IoT-based personal healthcare in smart spaces.* IEEE Internet of things journal, 1(2), 144-152.

Andročec, D., Picek, R., & Mijač, M. (2018). The Ontologically based Model for the Integration of the IoT and Cloud ERP Services. In *8th International Conference on Cloud Computing and Services Science (CLOSER 2018)*.

Ateeq, M., Ishmanov, F., Afzal, M. K., & Naeem, M. (2019). *Multi-parametric analysis of reliability and energy consumption in IoT: A deep learning approach.* Sensors, 19(2), 309.

Bahssas, D. M., AlBar, A. M., & Hoque, M. R. (2015). *Enterprise resource planning (ERP) systems: design, trends and deployment.* The International Technology Management Review, 5(2), 72-81.

Baker, S. B., Xiang, W., & Atkinson, I. (2017). *Internet of things for smart healthcare: Technologies, challenges, and opportunities*. IEEE Access, 5, 26521-26544.

Balampanis, S., Sotiriadis, S., & Petrakis, E. G. (2016). *Internet of things architecture for enhanced living environments.* IEEE Cloud Computing, 3(6), 28-34.

Barcelo, M., Correa, A., Llorca, J., Tulino, A. M., Vicario, J. L., & Morell, A. (2016). *IoT-cloud service optimization in next generation smart environments.* IEEE Journal on Selected Areas in Communications, 34(12), 4077-4090.

Bertino, E., Choo, K. K. R., Georgakopolous, D., & Nepal, S. (2016). *Internet of things (iot): Smart and secure service delivery*. ACM Transactions on Internet Technology (TOIT), 16(4), 22.

Brous, P., Janssen, M., & Herder, P. (2019). *The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations.* International

Journal of Information Management.
Bu, F., & Wang, X. (2019). *A smart agriculture IoT system based on deep reinforcement learning.* Future Generation Computer Systems, *99*, 500-507.
Bu, L., Isakov, M., & Kinsy, M. A. (2019). *A secure and robust scheme for sharing confidential information in IoT systems.* Ad Hoc Networks, 92, 101762.
Cai, H., Xu, B., Jiang, L., & Vasilakos, A. V. (2016). *IoT-based big data storage systems in cloud computing: perspectives and challenges.* IEEE Internet of Things Journal, 4(1), 75-87.
Caro, F., & Sadr, R. (2019). *The Internet of Things (IoT) in retail: Bridging supply and demand.* Business Horizons, 62(1), 47-54.
Celik, Z. B., Fernandes, E., Pauley, E., Tan, G., & McDaniel, P. (2018). *Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities.* arXiv preprint arXiv:1809.06962.
Chatterjee, U., Chakraborty, R. S., & Mukhopadhyay, D. (2017). *A PUF-based secure communication protocol for IoT.* ACM Transactions on Embedded Computing Systems (TECS), *16*(3), 67.
Chauhan, J., Rajasegaran, J., Seneviratne, S., Misra, A., Seneviratne, A., & Lee, Y. (2018). *Performance Characterization of Deep Learning Models for Breathing-based Authentication on Resource-Constrained Devices.* Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, *2*(4), 158.
Chen, X., & Hao, X. (2019). *Feature Reduction Method for Cognition and Classification of IoT Devices Based on Artificial Intelligence.* IEEE Access, 7, 103291-103298.
Choi, C., & Choi, J. (2019). *Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service.* IEEE Access, 7, 110510-110517.
Chowdhury, A., Raut, S. A., & Narman, H. S. (2019). *DA-DRLS: Drift adaptive deep reinforcement learning based scheduling for IoT resource management.* Journal of Network and Computer Applications, 138, 51-65.
Cui, L., Yang, S., Chen, F., Ming, Z., Lu, N., & Qin, J. (2018). *A survey on application of machine learning for Internet of Things.* International Journal of Machine Learning and Cybernetics, *9*(8), 1399-1417.
Daniel Snellman, *Difference in Cloud ERP Systems – A comparison, Degree Project In Information and Communication Technology*, Second Cycle, 30 Credits Stockholm, Sweden 2017.
Dawe, S. N., & Paradice, D. (2016). *A Systems Approach to Smart City Infrastructure: A Small City Perspective.* Dublin, Ireland, 11.
Deng, L., Li, D., Yao, X., Cox, D., & Wang, H. (2018). *Mobile network intrusion detection for IoT system based on transfer learning algorithm.* Cluster Computing, 1-16.
Elmonem, M. A. A., Nasr, E. S., & Geith, M. H. (2016). *Benefits and challenges of cloud ERP systems–A systematic literature review*. Future Computing and Informatics Journal, *1*(1-2), 1-9.
Emami Naeini, P., Degeling, M., Bauer, L., Chow, R., Cranor, L. F., Haghighat, M. R., &

Patterson, H. (2018). *The Influence of Friends and Experts on Privacy Decision Making in IoT Scenarios.* Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 48.

Fang, S., Da Xu, L., Zhu, Y., Ahati, J., Pei, H., Yan, J., & Liu, Z. (2014). *An integrated system for regional environmental monitoring and management based on internet of things*. IEEE Transactions on Industrial Informatics, *10*(2), 1596-1605.

Felemban, M., Felemban, E., Kobes, J., & Ghafoor, A. (2019). *Threat Management in Data-centric IoT-Based Collaborative Systems.* ACM Transactions on Internet Technology (TOIT), *19*(3), 42.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). *A Review on the Use of Blockchain for the Internet of Things.* IEEE Access, 6, 32979-33001.

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). *Evaluating critical security issues of the IoT world: Present and future challenges.* IEEE Internet of Things Journal, *5*(4), 2483-2495.

Georgakopoulos, D., Jayaraman, P. P., Fazia, M., Villari, M., & Ranjan, R. (2016). *Internet of Things and edge cloud computing roadmap for manufacturing*. IEEE Cloud Computing, (4), 66-73.

Gharaibeh, A., Khreishah, A., Mohammadi, M., Al-Fuqaha, A., Khalil, I., & Rayes, A. (2017). *Online auction of cloud resources in support of the Internet of Things*. IEEE Internet of Things Journal, *4*(5), 1583-1596.

Gogineni, S. K., Riedelsheimer, T., & Stark, R. (2019). *Systematic product development methodology for customizable IoT devices.* Procedia CIRP, *84*, 393-399.

Gonzalez-Manzano, L., Fuentes, J. M. D., & Ribagorda, A. (2019). *Leveraging User-related Internet of Things for Continuous Authentication: A Survey*. ACM Computing Surveys (CSUR), *52*(3), 53.

Guan, Z., Li, J., Wu, L., Zhang, Y., Wu, J., & Du, X. (2017). *Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid*. IEEE Internet of Things Journal, *4*(6), 1934-1944.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). *Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29*(7), 1645-1660.

Ham, S., Lee, J., & Lee, K. (2017). *QuickTalk: An Association-Free Communication Method for IoT Devices in Proximity*. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, *1*(3), 56.

Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). *Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches.* Internet of Things, *7*, 100059.

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). *Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions.* Future Generation Computer Systems, 97, 512-529.

Hossain, M. S., Rahman, M., Sarker, M. T., Haque, M. E., & Jahid, A. (2019). *A smart IoT based system for monitoring and controlling the sub-station equipment.* Internet of Things, 7, 100085.

Hu, C., Bao, W., Wang, D., Qian, Y., Zheng, M., & Wang, S. (2018). *sTube+: an IoT communication sharing architecture for smart after-sales maintenance in buildings.* ACM Transactions on Sensor Networks (TOSN), *14*(3-4), 29.

Huang, J., Kong, L., Chen, G., Wu, M. Y., Liu, X., & Zeng, P. (2019). *Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism*. IEEE Transactions on Industrial Informatics.

Huang, X., Hong, S. H., & Li, Y. (2017). *Hour-ahead price based energy management scheme for industrial facilities.* IEEE Transactions on Industrial Informatics, 13(6), 2886-2898.

Islam, M. M., Funabiki, N., Sudibyo, R. W., Munene, K. I., & Kao, W. C. (2019). *A dynamic access-point transmission power minimization method using PI feedback control in elastic WLAN system for IoT applications.* Internet of Things, *8*, 100089.

Jabbar, W. A., Shang, H. K., Hamid, S. N., Almohammedi, A. A., Ramli, R. M., & Ali, M. A. (2019). *IoT-BBMS: Internet of Things-Based Baby Monitoring System for Smart Cradle.* IEEE Access, *7*, 93791-93805.

Junior, C. M. D., da Silva, S. P., da Nóbrega, R. V., Barros, A. C., Sangaiah, A. K., Rebouças Filho, P. P., & de Albuquerque, V. H. C. (2019). *A new approach for mobile robot localization based on an online IoT system.* Future Generation Computer Systems.

Kamilaris, A., & Pitsillides, A. (2016). *Mobile phone computing and the internet of things: A survey.* IEEE Internet of Things Journal, 3(6), 885-898.

Karimanzira, D., & Rauschenbach, T. (2019). *Enhancing aquaponics management with IoT-based Predictive Analytics for efficient information utilization.* Information Processing in Agriculture.

Khan, M. A., & Salah, K. (2018). *IoT security: Review, blockchain solutions, and open challenges.* Future Generation Computer Systems, 82, 395-411.

Khelifi, H., Luo, S., Nour, B., Sellami, A., Moungla, H., Ahmed, S. H., & Guizani, M. (2018). *Bringing deep learning at the edge of information-centric Internet of Things*. IEEE Communications Letters, *23*(1), 52-55.

Ko, I. Y., Ko, H. G., Molina, A. J., & Kwon, J. H. (2016). *SoIoT: Toward a user-centric IoT-based service framework.* ACM Transactions on Internet Technology (TOIT), *16*(2), 8.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). *DDoS in the IoT: Mirai and other botnets.* Computer, 50(7), 80-84.

Konstantinidis, A., Irakleous, P., Georgiou, Z., Zeinalipour-Yazti, D., & Chrysanthis, P. K. (2018). *IoT Data Prefetching in Indoor Navigation SOAs.* ACM Transactions on Internet Technology (TOIT), 19(1), 10.

Kumrai, T., Ota, K., Dong, M., Kishigami, J., & Sung, D. K. (2016). *Multiobjective optimization in cloud brokering systems for connected Internet of Things.* IEEE Internet of things journal, *4*(2), 404-413.

Laput, G., & Harrison, C. (2019). *Exploring the Efficacy of Sparse, General-Purpose Sensor Constellations for Wide-Area Activity Sensing*. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, *3*(2), 55.

Lee, S. Y., Wi, S. R., Seo, E., Jung, J. K., & Chung, T. M. (2017). *ProFiOt: Abnormal Behavior Profiling (ABP) of IoT devices based on a machine learning approach.* In 2017 27th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1-6). IEEE.

Lenart, A. (2011). *ERP in the Cloud–Benefits and Challenges. In Euro Symposium on systems analysis and design*(pp. 39-50). Springer, Berlin, Heidelberg.

Li, H., Dong, M., & Ota, K. (2015). *Radio access network virtualization for the social Internet of Things.* IEEE Cloud Computing, 2(6), 42-50.

Li, H., Ota, K., & Dong, M. (2018). *Learning IoT in edge: Deep learning for the Internet of Things with edge computing*. IEEE Network, 32(1), 96-101.

Li, J., Siddula, M., Cheng, X., Cheng, W., Tian, Z., & Li, Y. (2019). *Approximate data aggregation in sensor equipped IoT networks.* Tsinghua Science and Technology, *25*(1), 44-55.

Li, Z., Guo, H., Wang, W. M., Guan, Y., Barenji, A. V., Huang, G. Q., & Chen, X. (2019). *A blockchain and automl approach for open and automated customer service.* IEEE Transactions on Industrial Informatics.

Liu, W., Zhang, L., Zhang, Z., Gu, C., Wang, C., O'neill, M., & Lombardi, F. (2019). *XOR-based low-cost Reconfigurable PUFs for IoT Security.* ACM Transactions on Embedded Computing Systems (TECS), *18*(3), 25.

Lv, P., Wang, L., Zhu, H., Deng, W., & Gu, L. (2019). *An IoT-Oriented Privacy-Preserving Publish/Subscribe Model Over Blockchains.* IEEE Access, *7*, 41309-41314.

Mahmud, B. (2017). *Internet of Things (IoT) for Manufacturing Logistics on SAP ERP Applications.* Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(2-6), 43-47.

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). *Big IoT data analytics: architecture, opportunities, and open research challenges.* IEEE Access, 5, 5247-5261.

Mary Sumner, (2014), Pearson New International Edition, British Library Cataloguing-in-Publication Data.

Meddeb, M., Dhraief, A., Belghith, A., Monteil, T., Drira, K., & Mathkour, H. (2019). *Least fresh first cache replacement policy for NDN-based IoT networks.* Pervasive and Mobile Computing, *52*, 60-70.

Metzger, F., Hoßfeld, T., Bauer, A., Kounev, S., & Heegaard, P. E. (2019). *Modeling of aggregated IoT traffic and its application to an IoT cloud.* Proceedings of the IEEE, 10*7*(4), 679-694.

Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). *Deep learning for IoT big data and streaming analytics: A survey*. IEEE Communications Surveys & Tutorials, 20(4), 2923-2960.

Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., & Imran, M. (2019). *Securing IoTs in distributed blockchain: Analysis, requirements and open issues.* Future Generation

Computer Systems, 100, 325-343.
Monk, E., & Wagner, B. (2012). Concepts in enterprise resource planning. *Cengage Learning*.
Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). *SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways.* Procedia Computer Science, 52, 452-459.
Muñuzuri, J., Onieva, L., Cortés, P., & Guadix, J. (2019). *Using IoT data and applications to improve port-based intermodal supply chains.* Computers & Industrial Engineering.
Nawaz, F., Janjua, N. K., & Hussain, O. K. (2019). *PERCEPTUS: Predictive complex event processing and reasoning for IoT-enabled supply chain.* Knowledge-Based Systems.
Novo, O. (2018). *Blockchain meets IoT: An architecture for scalable access management in IoT.* IEEE Internet of Things Journal, 5(2), 1184-1195.
Novo, O. (2019). *Making Constrained Things Reachable: A Secure IP-Agnostic NAT Traversal Approach for IoT.* ACM Transactions on Internet Technology (TOIT), *19*(1), 3.
Okafor, N. U., & Delaney, D. (2019). *Considerations for system design in IoT-based autonomous ecological sensing.* Procedia Computer Science, 155, 258-267.
Omitola, T., & Wills, G. (2018). *Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain.* Procedia Computer Science, *126*, 441-450.
Pan, C., Xie, M., Han, S., Mao, Z. H., & Hu, J. (2019). *Modeling and Optimization for Self-powered Non-volatile IoT Edge Devices with Ultra-low Harvesting Power.* ACM Transactions on Cyber-Physical Systems, 3(3), 32.
Pawlick, J., & Zhu, Q. (2017). *Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control.* IEEE Transactions on Information Forensics and Security, 12(12), 2906-2919.
Peña, M. A. L., & Fernández, I. M. (2019). *SAT-IoT: An architectural model for a high-performance fog/edge/cloud IoT platform.* In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (pp. 633-638). IEEE.
Perera, C., Liu, C., Ranjan, R., Wang, L., & Zomaya, A. Y. (2016). *Privacy-knowledge modeling for the internet of things: A look back. Computer*, *49*(12), 60-68.
Pourvahab, M., & Ekbatanifard, G. (2019). *An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology*. IEEE Access, 7, 99573-99588.
Randhawa, R. H., Hameed, A., & Mian, A. N. (2019). *Energy efficient cross-layer approach for object security of CoAP for IoT devices.* Ad Hoc Networks, *92,* 101761.
Rashid, M. A., Hossain, L., & Patrick, J. D. (2002). *The evolution of ERP systems: A historical perspective.* In Enterprise Resource Planning: Solutions and Management (pp. 35-50). IGI Global.
Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). *A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology.* Ad Hoc Networks, 101933.
Rathore, M. M., Paul, A., Ahmad, A., Anisetti, M., & Jeon, G. (2017). *Hadoop-based intelligent care system (hics): Analytical approach for big data in iot.* ACM Transactions on Internet Technology (TOIT), *18*(1), 8.

Restuccia, F., D'Oro, S., & Melodia, T. (2018). *Securing the internet of things in the age of machine learning and software-defined networking. IEEE Internet of Things Journal*, *5*(6), 4829-4842.

Rholam, O., & Tabaa, M. (2019). *Smart Device for Multi-band Industrial IoT Communications.* Procedia Computer Science, *155*, 660-665.

Saheb, T., & Izadi, L. (2019). *Paradigm of IoT Big Data Analytics in Healthcare Industry: A Review of Scientific literature and Mapping of Research Trends.* Telematics and Informatics.

Samie, F., Bauer, L., & Henkel, J. (2019). *From Cloud Down to Things: An Overview of Machine Learning in Internet of Things.* IEEE Internet of Things Journal.

Santoso, F. K., & Vun, N. C. (2015, June). *Securing IoT for smart home system.In 2015 International Symposium on Consumer Electronics (ISCE) (*pp. 1-2). IEEE.

Saxena, N., Grijalva, S., & Chaudhari, N. S. (2016). *Authentication protocol for an IoT-enabled LTE network.* ACM Transactions on Internet Technology (TOIT), 16(4), 25.

Sha, K., Yang, T. A., Wei, W., & Davari, S. (2019). *A survey of edge computing based designs for security.* Digital Communications and Networks.

Sharma, S. K., & Wang, X. (2017). *Live data analytics with collaborative edge and cloud processing in wireless IoT networks*. IEEE Access, 5, 4621-4635.

Shen, S., Huang, L., Zhou, H., Yu, S., Fan, E., & Cao, Q. (2018). *Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based IoT networks.* IEEE Internet of Things Journal, 5(2), 1043-1054.

Shevtsov, S., Weyns, D., & Maggio, M. (2019). *SimCA*: A control-theoretic approach to handle uncertainty in self-adaptive systems with guarantees.* ACM Transactions on Autonomous and Adaptive Systems (TAAS), *13*(4), 17.

Shih, C. S., Chou, J. J., Reijers, N., & Kuo, T. W. (2016). *Designing CPS/IoT applications for smart buildings and cities.* IET Cyber-Physical Systems: Theory & Applications, 1(1), 3-12.

Siboni, S., Shabtai, A., Tippenhauer, N. O., Lee, J., & Elovici, Y. (2016). *Advanced security testbed framework for wearable IoT devices.* ACM Transactions on Internet Technology (TOIT), *16*(4), 26.

Siddiqui, F., Beley, J., Zeadally, S., & Braught, G. (2019). Secure and lightweight communication in heterogeneous IoT environments. *Internet of Things*, 100093.

Siegemund, G., & Turau, V. (2018). *A self-stabilizing publish/subscribe middleware for iot applications.* ACM Transactions on Cyber-Physical Systems, *2*(2), 12.

Siryani, J., Tanju, B., & Eveleigh, T. J. (2017). *A machine learning decision-support system improves the internet of things' smart meter operations.* IEEE Internet of Things Journal, 4(4), 1056-1066.

Snellman, D. (2017). *Difference in Cloud ERP Systems: A comparison.*

Soliman, S., Jaela, M. A., Abotaleb, A. M., Hassan, Y., Abdelghany, M. A., Abdel-Hamid, A. T&Mostafa, H. (2019). FPGA implementation of dynamically reconfigurable IoT security module using algorithm hopping. *Integration*.

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964-975.

Strohbach, M., Ziekow, H., Gazis, V., & Akiva, N. (2015). Towards a big data analytics framework for IoT and smart city applications. In *Modeling and processing for next-generation big-data technologies* (pp. 257-282). Springer, Cham.

Subahi, A. F. (2019). *Edge-Based IoT Medical Record System: Requirements, Recommendations and Conceptual Design.* IEEE Access, *7*, 94150-94159.

Suman, S., & Pogarcic, I. (2017). *Development of ERP and other large business systems in the context of new trends and technologies.* International Journal Vallis Aurea, 3(2), 79-92.

Sun, M., Zhou, Z., Wang, J., Du, C., & Gaaloul, W. (2019). *Energy-efficient IoT service composition for concurrent timed applications.* Future Generation Computer Systems.

Sung, W. T., & Chiang, Y. C. (2012). *Improved particle swarm optimization algorithm for android medical care IoT using modified parameters*. Journal of medical systems, *36*(6), 3755-3763.

Tabrizi, F. M., & Pattabiraman, K. (2019). *Design-Level and Code-Level Security Analysis of IoT Devices.* ACM Transactions on Embedded Computing Systems (TECS), *18*(3), 20.

Tang, J., Sun, D., Liu, S., & Gaudiot, J. L. (2017). *Enabling deep learning on IoT devices. Computer, 50*(10), 92-96.

Tavanaa, M., & Hajipourc, V. (2019). *A practical review and taxonomy of fuzzy expert systems: methods and applications.* Benchmarking: An International Journal.

Tekeste, T., Saleh, H., Mohammad, B., & Ismail, M. (2018). *Ultra-Low Power QRS Detection and ECG Compression Architecture for IoT Healthcare Devices.* IEEE Transactions on Circuits and Systems I: Regular Papers, 66(2), 669-679.

Tello-Oquendo, L., Lin, S. C., Akyildiz, I. F., & Pla, V. (2019). *Software-Defined Architecture for QoS-Aware IoT Deployments in 5G Systems.* Ad Hoc Networks, 101911.

Tiloca, M., Nikitin, K., & Raza, S. (2017). *Axiom: DTLS-based secure IoT group communication.* ACM Transactions on Embedded Computing Systems (TECS), 16(3), 66.

Truong, H. L., & Dustdar, S. (2015). *Principles for engineering IoT cloud systems*. IEEE Cloud Computing, *2*(2), 68-76.

Ukil, A., Bandyopadhyay, S., & Pal, A. (2014). *IoT-privacy: To be private or not to be private.* In 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 123-124). IEEE.

Verdouw, C., Sundmaeker, H., Tekinerdogan, B., Conzon, D., & Montanaro, T. (2019). *Architecture framework of IoT-based food and farm systems: A multiple case study.* Computers and Electronics in Agriculture, 165, 104939.

Vögler, M., Schleicher, J. M., Inzinger, C., & Dustdar, S. (2016). *A scalable framework for provisioning large-scale IoT deployments.* ACM Transactions on Internet Technology (TOIT), *16*(2), 11.

Wang, A., & Guo, Y. (2019). *Multiple-Terminal Aggregation Algorithm for IoT Service.* Procedia

Computer Science, *147*, 495-498.

Wang, Q., Zhu, X., Ni, Y., Gu, L., & Zhu, H. (2019*). Blockchain for the iot and industrial iot: A review.* Internet of Things, 100081.

Wirtz, B. W., Weyerer, J. C., & Schichtel, F. T. (2019). *An integrative public IoT framework for smart government.* Government Information Quarterly, *36*(2), 333-345.

Wu, T., Redouté, J. M., & Yuce, M. R. (2018). *A wireless implantable sensor design with subcutaneous energy harvesting for long-term IoT healthcare applications.* IEEE Access, *6*, 35801-35808.

Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018*). IoT security techniques based on machine learning*. arXiv preprint arXiv:1801.06275.

Xu, S., Yang, G., Mu, Y., & Liu, X. (2019). *A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance*. Future Generation Computer Systems, 97, 284-294.

Yang, P., Stankevicius, D., Marozas, V., Deng, Z., Liu, E., Lukosevicius, A., & Min, G. (2016). *Lifelogging data validation model for internet of things enabled personalized healthcare.* IEEE Transactions on Systems, Man, and Cybernetics: Systems, *48*(1), 50-64.

Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., & Liu, W. (2011, July). *Study and application on the architecture and key technologies for IoT.* In 2011 International Conference on Multimedia Technology (pp. 747-751). IEEE.

Yao, H., Mai, T., Wang, J., Ji, Z., Jiang, C., & Qian, Y. (2019). *Resource Trading in Blockchain-based Industrial Internet of Things.* IEEE Transactions on Industrial Informatics.

Yıldırım, G., & Tatar, Y. (2018). *Simplified Agent-Based Resource Sharing Approach for WSN-WSN Interaction in IoT/CPS Projects.* IEEE Access, 6, 78077-78091.

Yin, J., Yang, Z., Cao, H., Liu, T., Zhou, Z., & Wu, C. (2019). *A Survey on Bluetooth 5.0 and Mesh: New Milestones of IoT.* ACM Transactions on Sensor Networks (TOSN), *15*(3), 28.

Zadeh, A. H., Akinyemi, B. A., Jeyaraj, A., & Zolbanin, H. M. (2018). *Cloud ERP Systems for Small-and-Medium Enterprises: A Case Study in the Food Industry*. Journal of Cases on Information Technology (JCIT), 20(4), 53-70.

Zheng, X., Martin, P., Brohman, K., & Da Xu, L. (2014). *Cloud service negotiation in internet of things environment: A mixed approach.* IEEE Transactions on Industrial Informatics, 10(2), 1506-1515.

Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). *Security and privacy for cloud-based IoT: Challenges.* IEEE Communications Magazine, 55(1), 26-33.

Zhou, L., Kondapalli, S. H., Aono, K., & Chakrabartty, S. (2019). *Desynchronization of Self-powered FN Tunneling Timers for Trust Verification of IoT Supply-chain*. IEEE Internet of Things Journal.

Zhu, H., Podesva, P., Liu, X., Zhang, H., Teply, T., Xu, Y., & Niculescu, A. (2019). *IoT PCR for Pandemic Disease Detection and Its Spread Monitoring.* Available at SSRN 3352008.

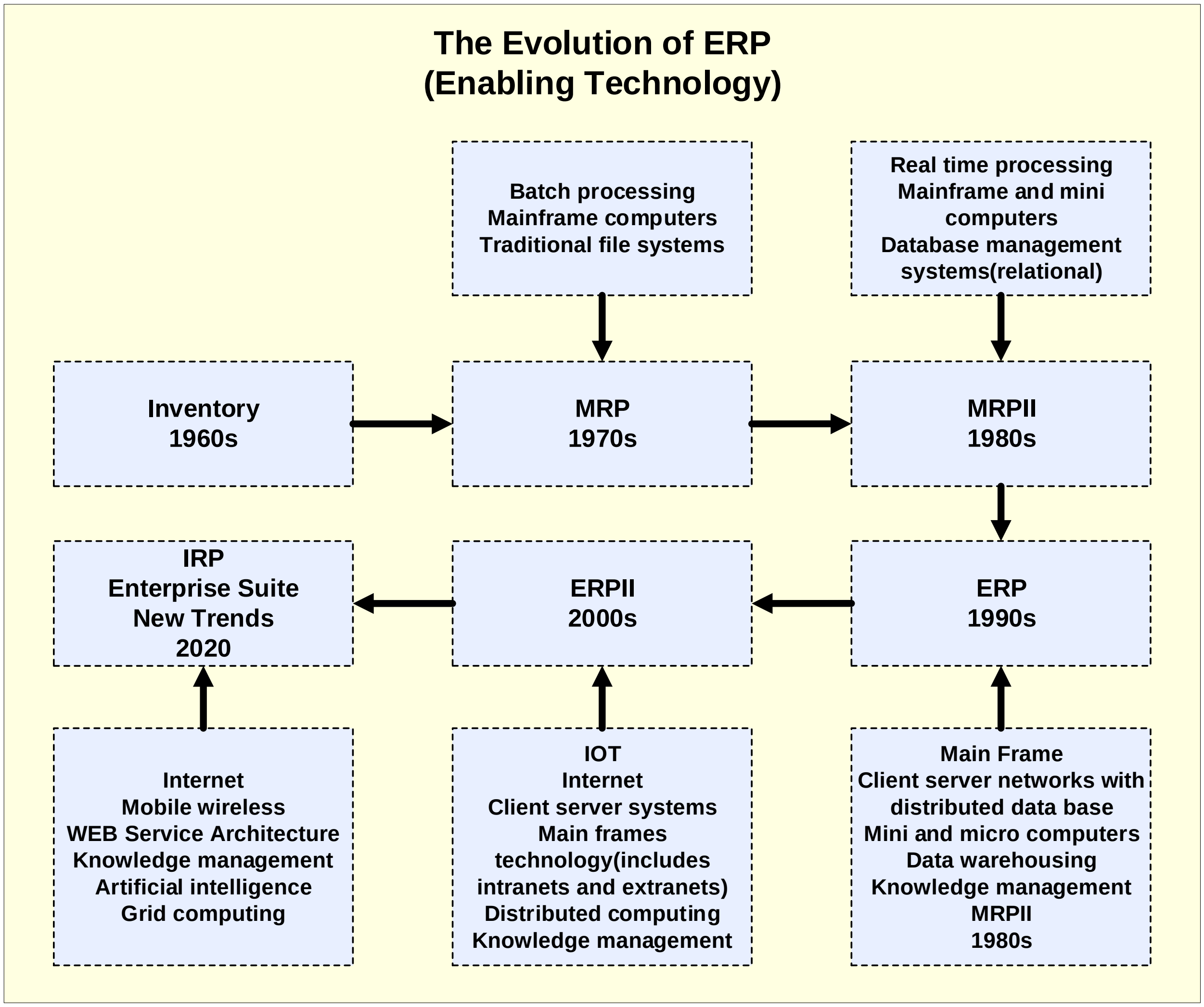

Figure 1. ERP evolution

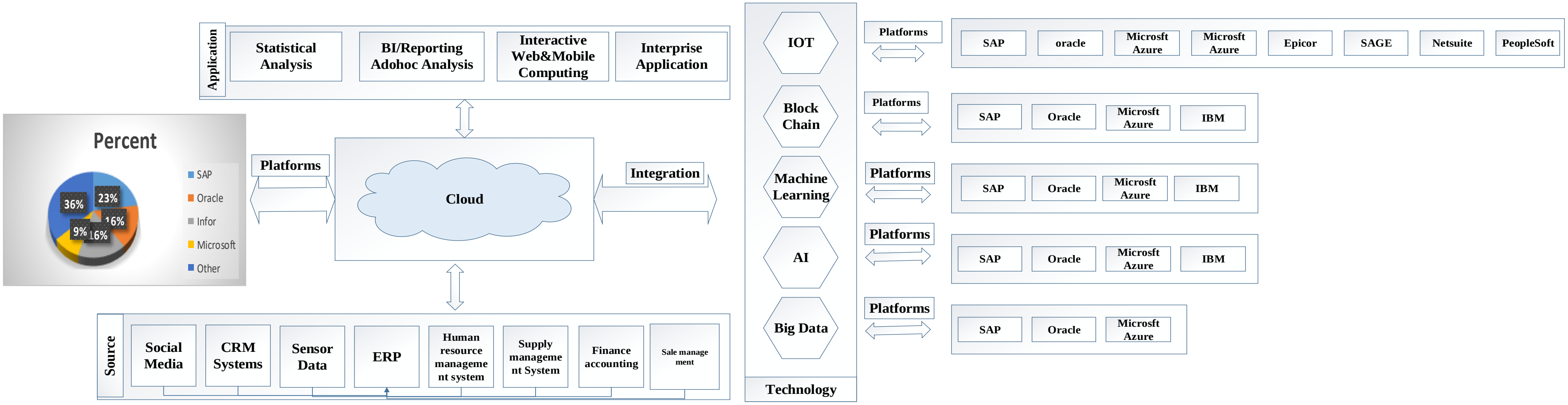

Figure 2. Cloud ERP, technologies, and platforms

Note: Some of the data presented in this figure are obtained from 2016 the Report on ERP Systems and Enterprise Software : A Panorama Consulting Solutions Research Report available at: https://www.panorama-consulting.com/wp-content/uploads/2016/07/2016-ERP-Report-2.pdf

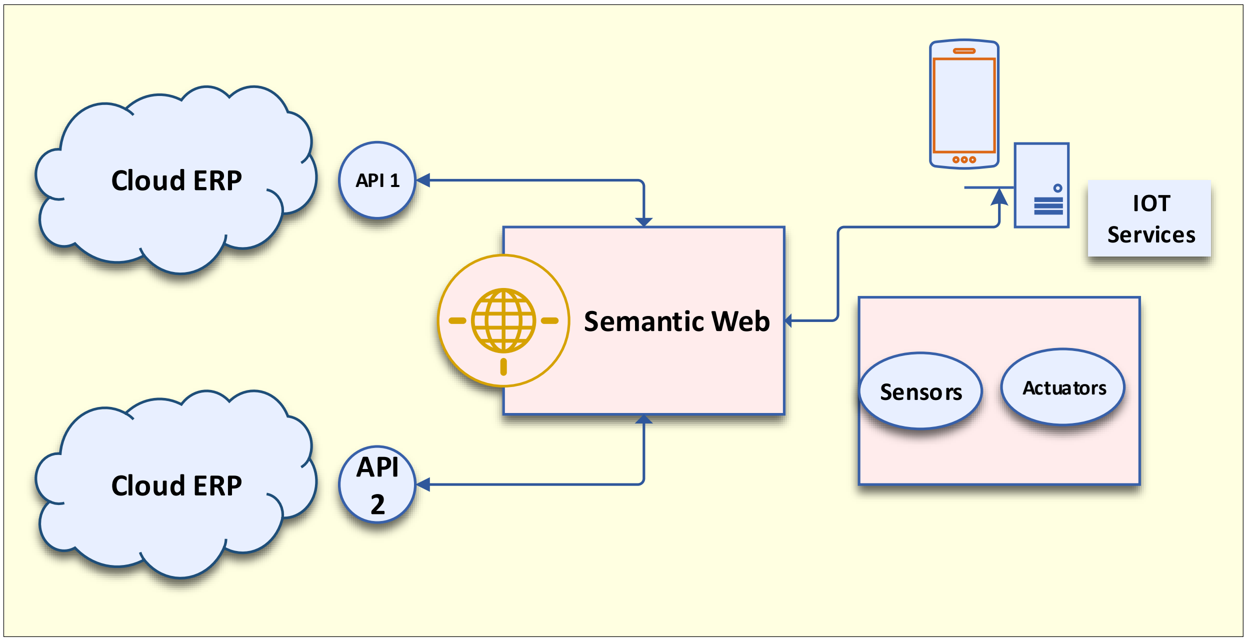

Figure 3. IoT and cloud ERP integration model

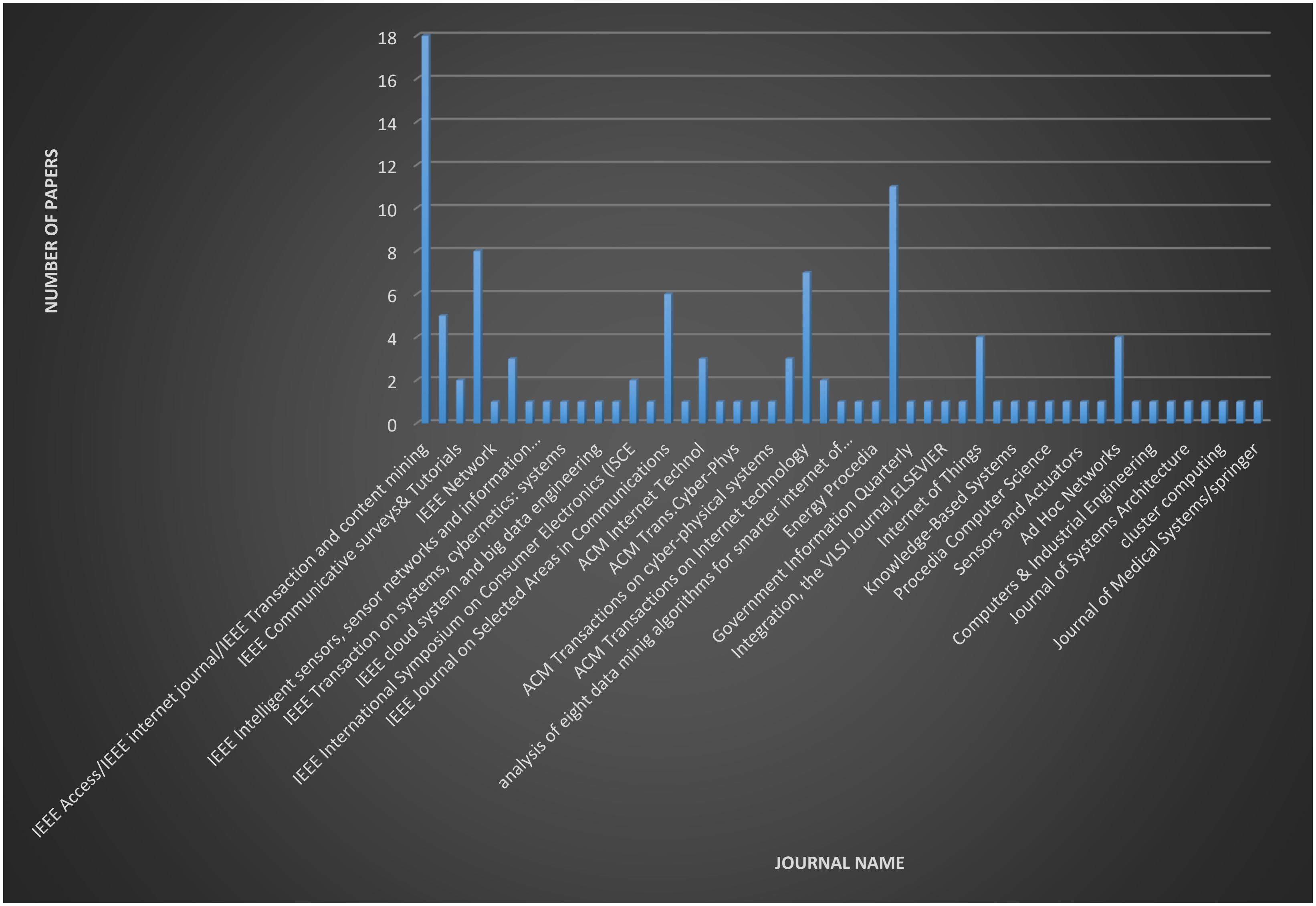

Figure 4. The papers published in each journal

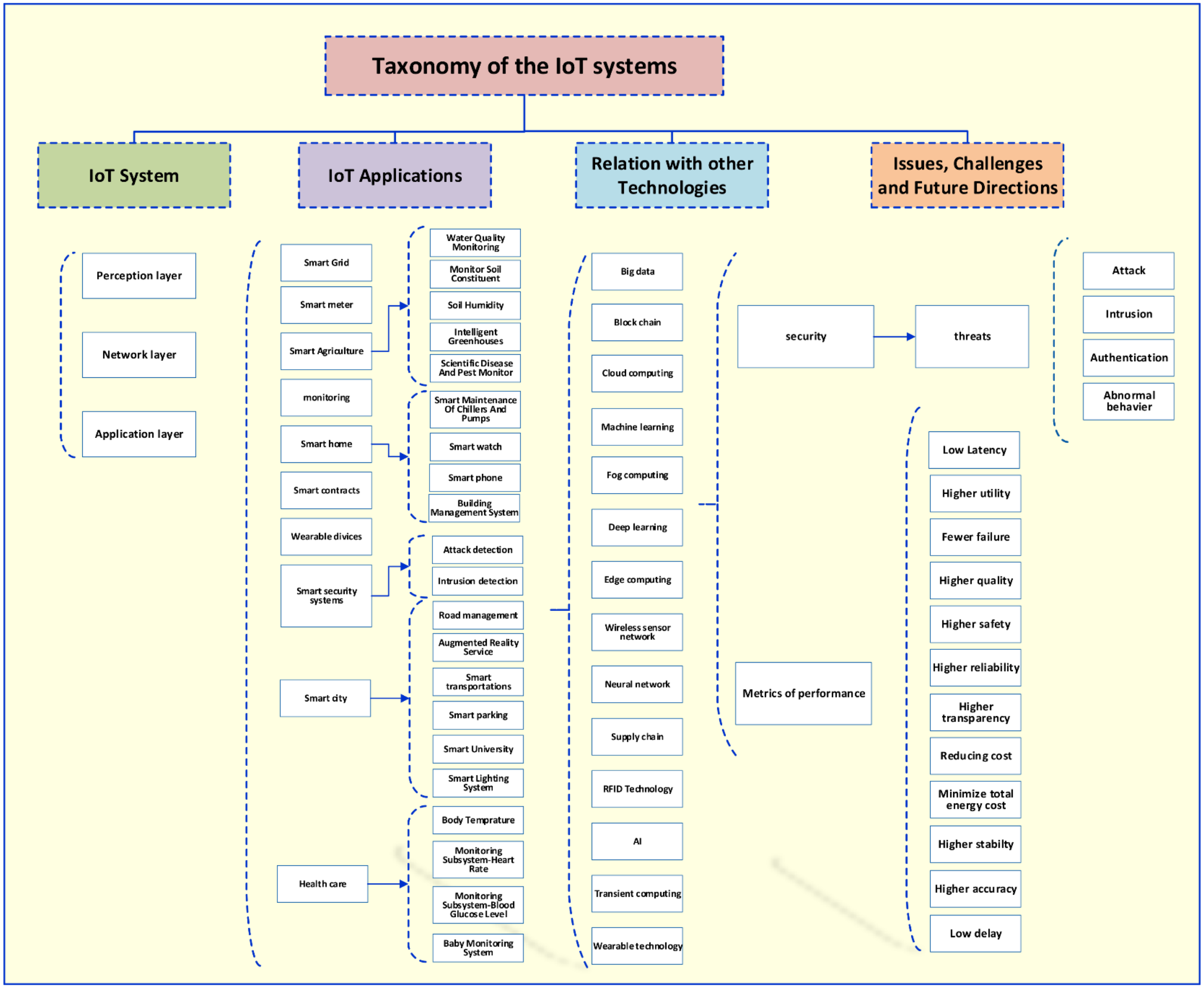

Figure 5. Taxonomy of IoT systems

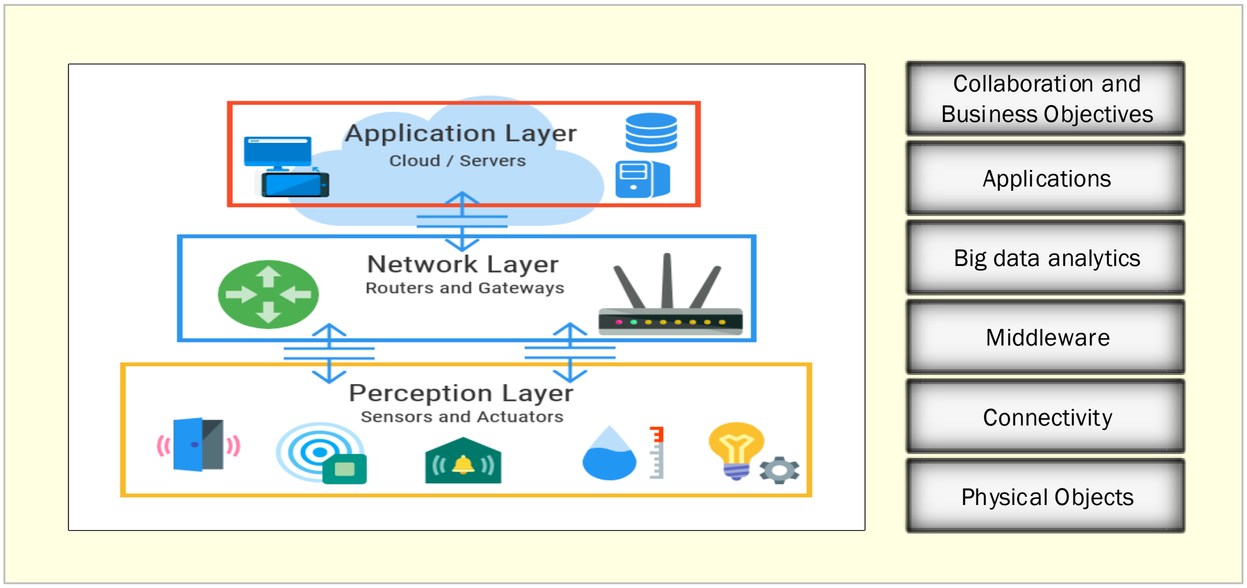

Figure 6. IoT system architecture

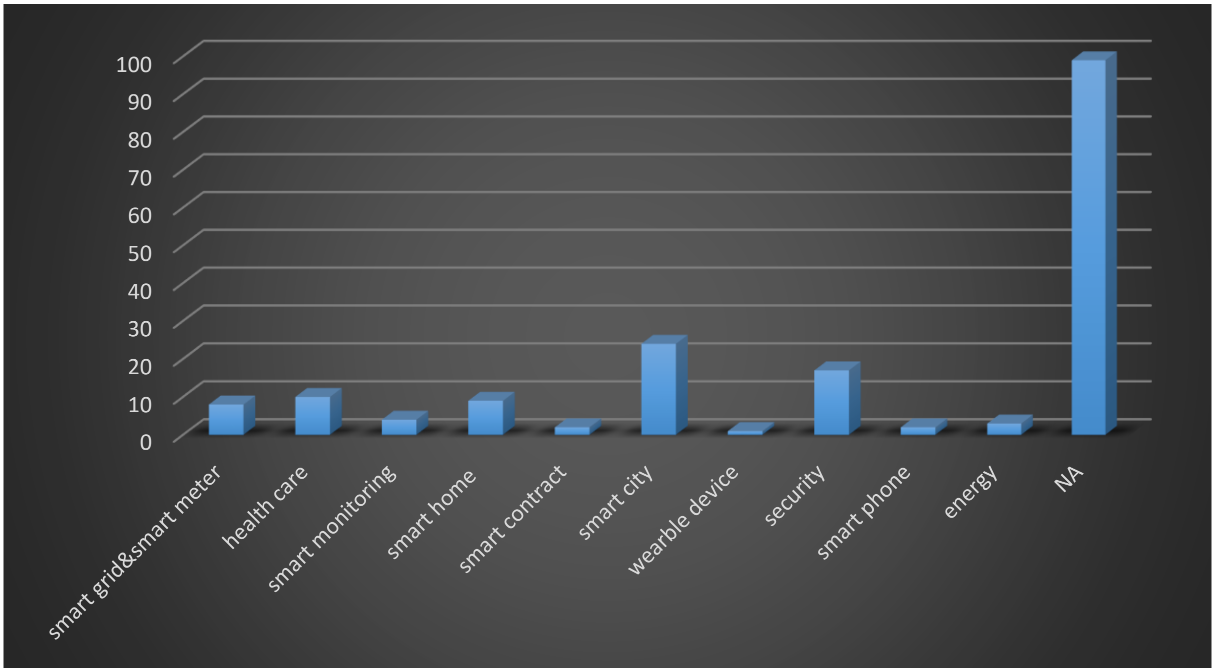

Figure 7. IoT applications

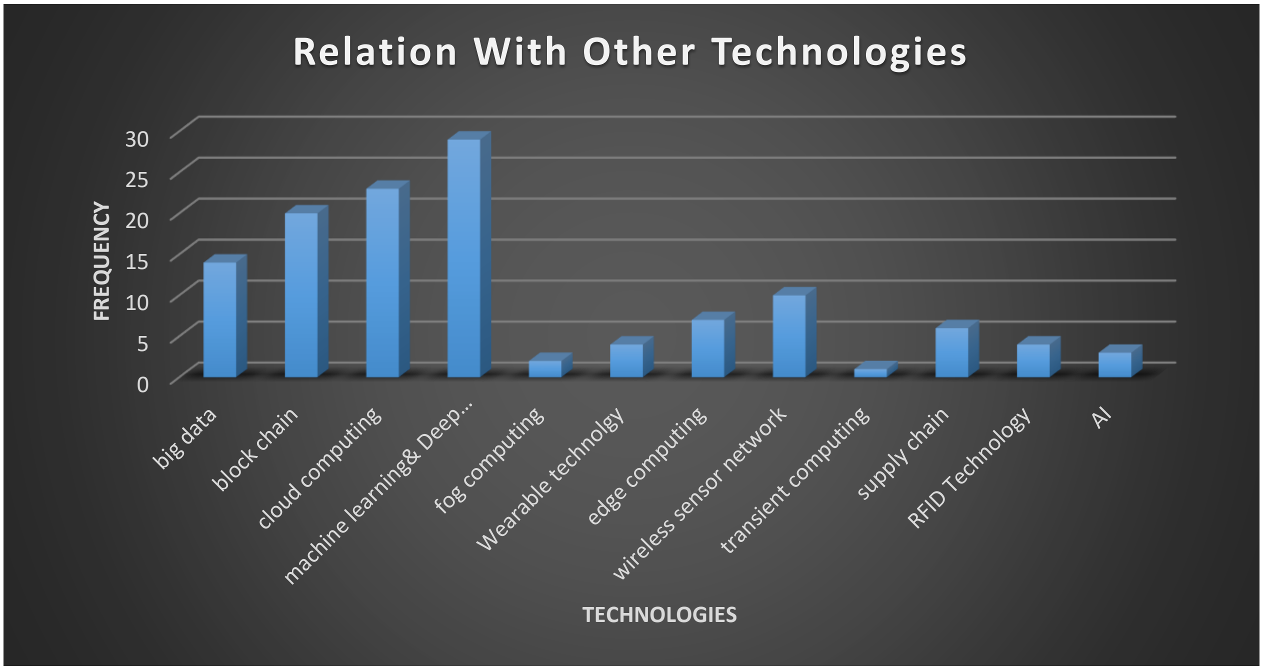

Figure 8. Relation with other technologies

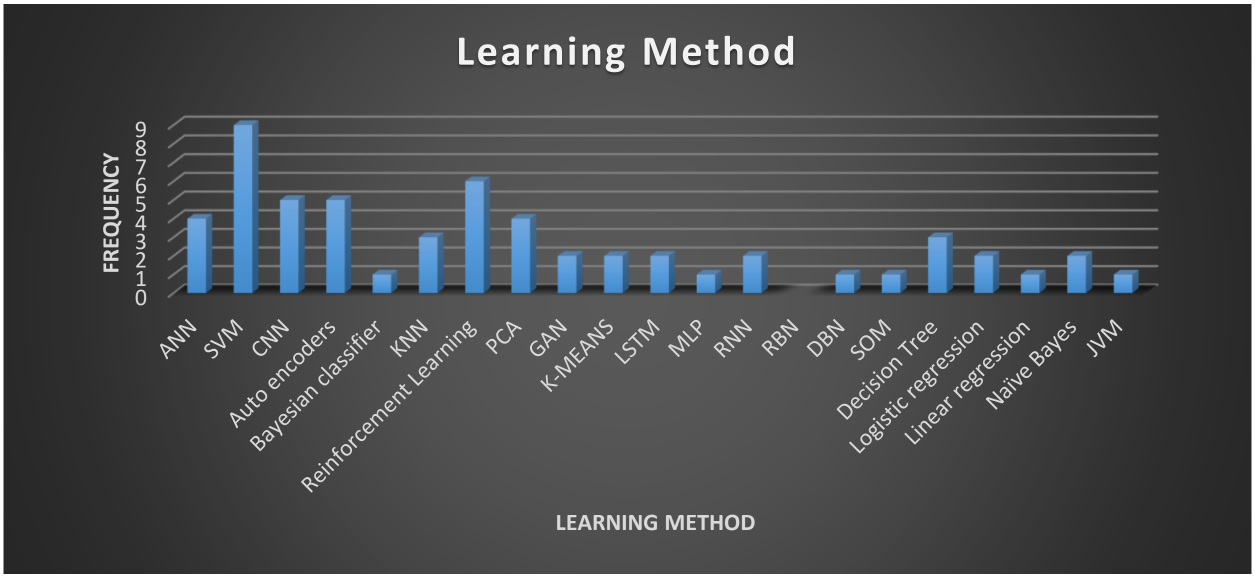

Figure 9. Learning methods

Table 1. ERP history

Type of System	Period	Goal	Systems
Reorder point systems	The 1960s	Available historical data is used to predict the expected inventory items in the future; when an item reaches a level less than the predetermined level, more products are ordered.	It is used to manage the production of some products in high volume and at constant demand; in these systems, the focus is on cost.
Material requirement planning system (MRP)	The 1970s	Provides a method based on the need for planning the production of products and ordering the raw materials	Focus on marketing; Emphasis on more Integration and planning
Manufacturing resource planning systems (MRP-II)	The 1980s	Planning the newly added capacity; can be used for planning and monitoring the implementation of production plans.	Focus on quality, focusing production strategy on process control, overhead costs reduction, and precise cost reporting.
Manufacturing execution systems (MES)	The 1990s	Enabling the adaptation of production plans to meet customer needs; providing more feedback in relation to sales activities	Focus on the ability to adapt new services and products on a timely basis to meet specific customer needs
Enterprise resource planning (ERP)	The late 1990s and beyond	Integrating the production process with supply chain processes in companies; designed to integrate enterprise business processes to provide a seamless flow of information from suppliers	Integrates supplier, manufacturer, and customer information throughout the supply chain.
IoT	1999	Everything has a digital identity and allows computers to organize and manage them.	The term "Internet of Things" was coined by Kevin Ashton, executive director of the Auto-ID Center

Table 2. Advantages and disadvantages of cloud ERP vs. on-premise ERP systems (+ ,-)

	Cloud ERP		On-Premise ERP	
Cost	+	• Costs identified over time • Inexpensive preliminary investment • Limited investment in hardware (e.g., server infrastructure)	-	• High risk of primary investment
	-	• High property costs over the entire system lifecycle	+	• Reduced initial system risk
Security	+	• Data is stored on vendor servers, and security is usually in the vendor's hand. • Prospect of continuing stability resulting in regular updates from the vendor as little customization is necessary.	-	• Providing the organization with data security may keep the data secure**.** • The runtime may be a function of customization**.**
	-	• While data security is in the hand of vendors, security is not fully guaranteed. In addition, prospects may not go well in some orGANizations.	+	• The data is stored on the customer's server, and security is usually provided by the orGANization.
Customization	+	• Facilitation of customization for its flexibility.	-	• Customization may lead to problems after a software update by the vendor
	-	• There are a few customization options.	+	• Facilitation of customization
Implementation	+	• Lower implementation time is needed.	-	• The implementation time sometimes lasts longer than usual.
	-	• Shorter implementation time may be a function of lower customization options.	+	• The enterprise exerts a higher level of control.

Table 3. IoT review articles

Paper	year	Brief description
A Review on the Use of Blockchain for the Internet of Things	2018	This paper presents a focus on the way blockchain is adapted to the specific needs of IoT in an attempt to develop Blockchain-based IoT (BIoT) applications. .
A Survey of Machine and Deep Learning Methods for the Internet of Things (IoT) Security	2018	this paper presents a comprehensive review of machine learning (ML) methods as well as the recent advances in the field, which can be deployed in the development of advanced security methods of IoT systems.
A survey on the application of machine learning for the Internet of Things	2018	This paper examines how machine learning works in the IoT domain intends to shed light on the recent advances in the IoT ML techniques and surveys of various IoT applications.
Deep Learning for IoT Big Data and Streaming Analytics: A Survey	2018	This paper focuses on Deep Learning (DL), i.e., a class of advanced ML in an attempt to smooth the learning process in the IoT domain. The authors in this paper mention the characteristics of IoT data and introduce two significant IoT data treatments, i.e., IoT big data analytics as well as IoT streaming data analytics.
Enabling Deep Learning on IoT Devices	2017	This paper looks into the integration of deep learning and low-potheyr IoT products. IoT-based devices are enabled by DL, and this helps them to render the unstructured multimedia data and be responsive no only to the environmental events but also to the users as well as the potheyr requirements.
Evaluating Critical Security Issues of the IoT World: Present and Future Challenges	2017	This paper focuses on three major layers of the IoT system model, namely, Perception, Transportation, and Application providing a taxonomic analysis from these three perspectives. The authors offer, in the end, the most critical issues as a guide for future research directions. .
Feature Reduction Method for Cognition and Classification of IoT Devices Based on Artificial Intelligence	2019	This paper explains the potheyr amplifier radio frequency (RF) fingerprinting as an example.The paper mainly focuses on studying the RF fingerprint dimension reduction method while taking into account the uncorrelated or redundant features as well as the high dimensionality of RF fingerprint features.
From Cloud Down to Things: An Overview of Machine Learning on the IoT	2019	This paper examines the role of machine learning plays in IoT, as well as the various functions of machine learning in application data processing and managerial tasks.
IoT for Smart Healthcare: Technologies, Challenges, and Opportunities	2017	This paper explains the most recent research on different areas of the model, taking into account their pros and cons and discusses whether the model can be fulfilling for a wearable IoT healthcare system.
IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges	2016	This paper introduces the research topics and publications which have been conducted in the domain of critical IoT application.
Mobile Phone Computing and the IoT: A Survey	2016	This paper provides a selection of more than 100 major up to date studies in the field. Based on their domain and area of application such as health, sports, gaming and etc., and the type of focus, whether it includes participatory sensing, eco-feedback, actuation, and control, and the involved communicating agent such as things or people, these papers are categorized to 10 domains.
		The paper also presents an analysis of the open issues and research gaps after they are identified.
Modeling of Aggregated IoT Traffic and Its Application to an IoT Cloud	2019	This paper provides an insight into the accuracy of the Poisson approximation model.
Securing the IoT in the Age of Machine Learning and Software-defined Networking	2018	In this paper, a taxonomy and a review of the most recent research on IoT security are provided while presenting a roadmap of the real research challenges of employing machine learning and software-defined networking to focus on the current and future IoT security issues.
Smart Electricity Meter Data Intelligence for Future Energy Systems: A Survey	2015	The focus of this paper is on the smart electricity meters along with their use while taking into account the significant aspects metering process, the benefits of the shareholders as well as the technologies dealing with the interests of the shareholders. The paper put the spotlight on the challenges as well as the opportunities brought about by the big data and the rising interest in cloud environments.
Survey of platforms for massive IoT	2018	This paper is devoted to IoT platforms focusing mainly on their components and features.
Data fusion and IoT for ubiquitous smart environments: A survey	2017	By focusing mainly on the mathematical methods, e.g., probabilistic methods, artificial intelligence, and theory of belief as well as particular IoT environments, e.g., distributed, heterogeneous, nonlinear, and object tracking environments, this paper presents a literature review of IoT data fusion.

Big IoT data analytics: architecture, opportunities, and open research challenges	2017	This paper proposes a state of the art architecture for big IoT data analytics after the most recent researches on the topic are examined, and the relation between IoT and big data analytics are explained.
"IoT (IoT): A vision, architectural elements, and future directions,	2017	This paper discusses the implementation of IoT across the world from the cloud-centric vision perspective.
Secure integration of IoT and cloud computing	2018	In this paper, IoT and cloud computing are examined while concentrating on the security issues of these two domains.
A survey: Attacks on RPL and 6LoWPAN in IoT	2015	This paper discusses the potential attacks on RPL as well as the 6LoWPAN network while examing the countermeasure against them and pointing out the consequences on network parameters.
Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities	2019	This paper provides a survey of the privacy and security challenges which demand program-analysis techniques in IoT focusing on the attacks which have been launched against these systems as well as the defense deployed against them.
Leveraging User-related IoT for Continuous Authentication: A Survey	2019	More than 58 papers on the major components, such as a CA system, are thoroughly examined in this paper. The paper also studies the industry status focusing on 32 market contributions, research projects, and related standards. .
Blockchain for the IoT and Industrial IoT: A review	2019	This paper starts with examing the underlying structure as well as the key features of blockchain and then focus on the security requirement for Industry 4.0 and IoT development. Finally, the paper investigates the way IoT security tools and techniques are employed to apply blockchain to IoT for industry 4.0.
A survey of edge computing-based designs for IoT security	2019	In an attempt to motivate edge-based IoT security designs, the present paper provides a thorough study of the current IoT security solutions.
Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges	2019	In this paper, after the OS standard features and hardware IoT platforms are explained, an OS-to-hardware architectures features-mapping is proposed focusing on the investigation of the unique requirements that IoT application has.
The dual effects of the IoT (IoT): A systematic review of the benefits and risks of IoT adoption by orGANizations	2019	This paper explains the advantage and disadvantages of IoT after analyzing its adaptation by the organizations. Actually, the advantages and disadvantages of the IoT are categorized into Big, Open, Linked Data (BOLD)as a result of a thorough review of the literature.
Privacy preservation in blockchain-based IoT systems: Integration issues, prospects, challenges, and future research directions	2019	In this paper, the integration of blockchain technology in IoT scenarios is analyzed, emphasizing the privacy challenges resulted from this integration.
The paradigm of IoT Big Data Analytics in Healthcare Industry: A Review of Scientific literature and Mapping of Research Trends	2019	This paper aims at examining the impacts of IoT Big Data Analytics paradigm (IoT BDA) on the implementation and application of IoT-based technologies in the area of healthcare services. A comprehensive review of the literature in the domain is presented, and the research trends are mapped onto the IoT BDAin the healthcare industry to achieve this. In fact,46 papers regarding IoT BDA, as well as 84 papers about fog computing in the healthcare industry, are reviewed from qualitative and quantitative perspectives in the paper.
Blockchain-based IoT: A Survey	2019	This paper presents a thorough examination of the BCoT by providing summarized explanations of what IoT is and what challenges it poses. Then, a brief review of the blockchain is presented to introduce the integration of blockchain with IoT, an attempt which led to a proposal regarding BCoT architecture.

Table 4. IoT applications

IoT application domain	Reference
Smart Grid& Smart meter	Guan (2017), Afzal et al. (2017), Siryani et al. (2017), Ukil et al. (2014), Tabrizi and Pattabiraman(2019), Marjani et al. (2017), Rholam and Tabaa (2019),
Health care	Taiyang Wu Jean et al. (2018), Subahi(2019), Baker et al.(2016), Yang(2016), Tekeste et al.(2018), Sra Amendola et al.(2014), Rathore et al.(2017), Afzal et al.(2017), Saheb and Izadi (2019), Zhu et al.(2019).
Smart Monitoring	Jabbar et al.(2016), Tekeste et al.(2018), Shevtsov et al. (2019), Md. Sanwar Hossain et al.(2016).
Smart Home (smartwatch, smartphone, smart building)	Fang et al. (2017), Laput and Harrison (2019), Chauhan et al. (2018), Tiloca et al. (2017), Laput and Harrison (2019), Saeed et al. (2016), SIBONI et al., (2016), Rholam and Tabaa (2019).
Smart Contract	Novo (2020), Dai et al. (2019).
Smart City(road management, smart agriculture, smart transportation, smart parking, smart university, smart building)	Marc Barcelo (2017), Florian Metzger et al. (2016), Ammar Gharaibeh et al. (2019), Choi and Choi (2017), Perera et al. (2015), Mohammadi et al. (2018), Martin Strohbach et al. (2016), Furqan Alam et al. (2017), Furqan Alam et al. (2016), Chuang Hu et al. (2018), Luca Calderonia et al. (2019), Paul Brous et al. (2019), Fanyu Bu and Xin Wang (2019), Shih et al. (2016), Celesti et al., (2014), Vogler et al. (2016), Alama et al., (2016), Baranwal et al. (2016), Marjani et al. (2017), Hu et al. (2018), Calderonia et al. (2019), Rholam and Tabaa (2019), Bu et al. (2018).
Wearable devices	Ren et al. (2017).
Security(Intrusion detection, Attack detection, Authentication)	Mahmudul Hasan et al. (2019), Ketheyi Sha et al. (2019), Adnan Akbar et al. (2017), Xiao et al. (2018), Chauhan et al. (2018), Saxena et al. (2016), Emami Naeini et al. (2018), Chatterjee et al. (2017), Tabrizi and Pattabiraman (2019), Shen et al. (2018), Li et al. (2019), Guan (2017), Siddiquia et al. (2017), Ratheea et al. (2019). Sha et al. (2019)
smartphone	Kamilaris & Pitsillides(2017), Chauhan et al.(2018)
Energy	Sun et al.(2019), Randhawa(2018), Pan et al. (2019).
Other	Rathee et al. (2019), Alahakoon and Yu (2015), Al-Garadi et al. (2018), Ateeq et al. (2019), Bertino et al. (2016), Bu et al. (2019), Cai et al. (2016), Caro and sadr (2019), Celik et al. (2018), Chen and Hao (2019), Chowdhury et al. (2019), Cui et al. (2018), Dawe& Paradice (2016), Deng et al. (2018), Naeini et al. (2018), Felemban et al. (2019), Fernández-Caramés & Fraga-Lamas (2019), Frustaci et al. (2017), Georgakopoulos et al. (2016), Gogineni et al. (2019), Gonzalez-Manzano et al. (2019), Gubbi et al. (2013), Ham et al. (2017), Hassan et al. (2019), Huang et al. (2019), Huang et al. (2017), Islam et al. (2019), Junior et al. (2019), Karimanzira and Rauschenbach (2019), Khan and Salah (2018), Khelifi et al. (2018), Ko et al. (2016), Kolias et al. (2017), Lee et al. (2017), Dong and Ota (2015), Ota and Dong (2018), Li et al. (2019), Liu et al. (2019), Lv et al. (2019), Meddeb et al. (2019), Moin et al. (2019), Moosavi et al. (2015), Muñuzuri et al. (2019), Nawaz et al. (2019), Nano (2018), Novo (2019), Okafor and Delaney (2019), Omitola and Wills (2018), Pawlick and Zhu (2017), Peña and Fernández (2019), Pourvahab and Ekbatanifard (2019), Restuccia et al. (2018), Samie and Bauer (2019), Sha et al. (2019), Sharma and Wang (2017), Siboni et al. (2016), Siddiqui et al. (2018), Siegemund and Turau (2018), Soliman et al. (2019), Stergiou et al. (2018), Sung & Chiang (2012), Tang et al. (2017), Tello-Oquendo et al. (2019), Truong and Dustdar (2015), Verdouw et al. (2019), Wang and Guo (2019), Wang et al. (2019), Wirtz et al. (2019), Wu et al. (2018), Xu et al. (2019), Yang et al. (2011), Yao et al. (2019), Yıldırım and Tatar (2018), Yin et al. (2019), Zheng et al. (2014), Zhou et al. (2017), Zhou et al. (2019),Yavuz (2018), Mahmud (2018), Balampanis et al.,(2016), Hongming et al.,(2017), Kumrai et al.,(2019), Andročec et al.,(2018), Wanga and Gue (2018), AhmadKhan and salah (2018), Chowdhury et al. (2018), Carlos et al. (2019), Gogineni et al. (2019), In-Young Ko et al., (2016), Ahmed Saeed et al. (2016), Konstantinidis et al., (2018), Manzano et al., (2019).

Table 5. Machine learning and deep learning methodsin IoT-based ERP

Method	Working principle	Advantages	Disadvantages	Application in IoT-based ERP/ methods reference
Decision Tree (DT)	• The DT-based approach uses DT to create a model (i.e., a forecast model) in which the training examples are considered as branches and leaves which facilitate the learning process. The new sample class is also predicted using the previously-learned model.	• It is actually a clear and simple method. • Data preparation during the pre-processing takes less effort in comparison with other algorithms. • No normalization is required for the DT. • No scaling of data is required. • The loss of values in the data has NO considerable effect on creating a decision tree. • It is easy to explain this tree to the team and the shareholders. In addition, it is an intuitive model.	• DT needs a lot of storage space because of its structural nature. DT-based approaches are easy to understand only if few DTs are involved. • The structure of the DT is very sensitive to the changes in the data. In fact, if the data changes a little, the structure undergoes a huge change causing instability. • In comparison with other algorithms, the calculations for a DT may become too complicated. • A decision tree often involves a longer time to train the model. • Decision tree training is relatively expensive because of higher complexity and longer time. • The algorithm of the DT is not accountable for applying regression and predicting continuous values.	• Intrusion detection and smart grid • Siryani et al. (2017), • Hasan et al. (2019)
Support Vector Machine (SVM)	• SVMs create a dividing highway in the feature dimension of two or more classes so that the distance between the highway and the adjacent sample points of each class is maximized.	• SVMs are generalizable and adequate for data with a lot of descriptive features and a few sample points. • Hyperline detects optimal segregation. • Maximizes the boundaries between different classes. • As for classes with a clear margin of separation, SVMs perform relatively well. • High dimensional spaces contribute to more efficiency of SVM. • When the number of dimensions is bigger than that of samples, SVM becomes effective. • SVM is somehow efficient from the memory perspective.	• An optimal choice of a core is a difficult task. Understanding and interpretation of SVM-based models are also difficult. • Its algorithm is not adequate for a large data set. • As for the data with more noise, SVM performance is not satisfactory. • The SVMs underperform when the number of features for each data point exceeds the number of training data samples. • Since the functionality of the support vector classifier depends in the data points, there is no probabilistic explanation for the classification above and below the classifying hyperplane.	• Attack detection, intrusion detection, smart city, malware detection, smart grid, and sensor network • Yildirim and Tatar (2018) • • Alama et al. (2016). • Chauhan et al. (2018). • Vogler et al. (2016). • Carlos et al. (2019).
Naïve Bayes (NB)	• NB calculates posterior probability. NB used Bayes theorem to predict the probability that a particular feature set of unlabeled specimens fits into a specific label assuming independence among features.	• It is fast, simple, and easy to use. • If the NB conditional independence assumption, then it will converge quicker than discriminative models like logistic regression. • Even if the NB assumption doesn't hold, it works great in practice. • It does not require a lot of training data. • It has high linear scalability with the number of predictors and data points. • It is applicable in both binary and multiclass classification problems. • It is capable of probabilistic predictions. • It is capable of handling continuous and discrete data. • Irrelevant features do not affect them.	• NB independent use of features makes it impossible for NB to capture useful clues from the relationships and interactions between features. • (NB may have a better performance in applications whose instances have dependent and related features.).	• smart city, smart grid// • Alama et al. (2016) • Siryani et al. (2017)

KNN	• The KNN classifies the new sample according to the votes of a select number of its closest neighbors. That is, the KNN class identifies unknown samples with the majority of votes to its nearest neighbors.	• KNN is a popular and efficient approach to detect intrusion. • Robust to noisy training data (especially if we use the inverse square of the weighted distance as the distance). • It becomes effective when there is a large amount of training data.	• The optimal value is usually different from one dataset to another. Therefore, determining the optimal value of K can be a challenging and time-consuming process. • Needs to specify the value of the k parameter (number of nearest neighbors). • It is inadequate for distance-based learning because the type of distance and attribute which must be used to derive the best results are not specified. • The high computation cost is necessary to compute the distance between each query instance and all training samples. However, indexing may be helpful in reducing this cost.	• Attack detection, malware detection// • Xiao et al. (2018) • Alama et al. (2016) • Carlos et al. (2019)
Random Forest (RF)	• In RF, several DTs are built and combined to achieve a well-established prediction model to improve overall results.	• RF is extremely resistant to overfitting. It avoids feature selection and needs only a few input parameters. • The overfitting of a single decision tree can be tackled by the process of averaging or combining the results of different decision trees. • RFs performs much better than a single DT when it comes to a huge amount of data items because they have less variance in comparison with a single DT. • They are very flexible and show high accuracy. • There is no need to prepare input data because the data do not need to be scaled. • Its accuracy remains the same in case of missing a large amount of data.	• RF is based on the construction of several DTs. Therefore, it may be impractical for specific online programs where the training data sets are large. • A critical problem with the RFs is that they are very complicated. In comparison with the DT, they are more difficult and time-consuming. • Because RF includes a lot of decision trees, it is less intuitive and demands more computational resources. This because the large number of the DTs makes it difficult to understand the relationship governing the input data. • In comparison with other algorithms, the prediction process becomes longer. •	• Hasan et al. (2019)
k-Means Clustering clustering	• In k-Means clustering is an unsupervised learning approach that identifies clusters of data with respect to the similarities of attributes and denotes the number of clusters created by the algorithm.	• Unsupervised algorithms are usually a good choice when it is difficult to generate labeled data. Clustering of K averages can be used to anonymize private data in an IoT system because it does not require labeled data. • It is easy to use. • In comparison with the hierarchical clustering, K-means may perform faster computations because of the large number of variables it includes (if K is small). • In comparison with the hierarchical clustering, K-Means may produce higher clusters. • After the centroids are recomputed, an instance can move to another cluster.	• The clustering of k-means is less effective than supervised learning methods, especially in identifying known attacks. • Predicting the number of clusters (K-Value) is difficult. • The final results are deeply affected by the initial seeds. • The final results get affected by order of the data. • Another disadvantage of the K-Means is that it is sensitive to scale. In other words, if you normalize, standardize, or rescale your datasets, your results will change drastically. Although this is not a disadvantage in itself, nit being aware of the extra time needed to scale the data is annoying.	• Deng et al. (2018)

Principal Component Analysis (PCA)	• NB PCA is a process that converts a number of possibly correlated features into a smaller number of unrelated features, called core components.	• PCA can lead to dimensional reduction and mitigation of the model complexity. • It's very efficient. • It is based on a hierarchy arranged according to the relevance. • Its performance is excellent for most data sets.	• In order to have high efficiency, the PCA, which is a technique for feature reduction, needs to be used in conjunction with the machine learning methods. • The performance of PCA depends highly on the non-linearity of the data. • Results are not always the best for visualization • Rendering it is difficult • It is capable of discarding useful information because it is too focused on the variance, while sometimes there is not a direct link between the variance and the predictive power.	• Yildirim and Tatar (2018) • Deng et al. (2018)
SOM	• SOM is a kind of artificial neural network (ANN) which used for dimensionality reduction. It is trained using unsupervised learning to produce a low-dimensional (typically two-dimensional), discretized representation of the input space of the training samples named a map.	• It transforms high dimensional data to lower-dimensional mao • It contributes to mapping the similar objects onto the locations adjacent to them on the map by maintaining the topological properties of the input space. • It can be efficiently used for visualization. • It contributes to the topology relations in the input space.	• Clustering result depends on the initial weight vector • It demands a lot of good training data. • It is difficult to specify the best map size • High computation cost	• Yildirim and Tatar (2018)
A multilayer perceptron (MLP)	• MLP tends to tackle problems that demand supervised learning, and it is also employed in researches on computational neuroscience and parallel distributed processing.	• Guarantee of the possibility of solving of tasks	• Low speed of learning • Possibility of overfitting • Impossible to relearning • Selection of structure needed for solving of a concrete task I unknown	• Huang et al. (2017) • Chauhan et al. (2018)
Bayesian network(BN)	• BN is a probabilistic graphical model that uses a directed acyclic graph (DAG) to provide a set of variables as well as their conditional dependencies. It actually considers an event that takes place to predict the weather; the contributing factor is one of the several possible known causes.	• It can readily handle incomplete data sets • It Allows Ine To Learn About Causal Relationships. • It readily facilitates the use of prior knowledge.	• It is more complex to construct the graph.	• Carlos et al. (2019)
ANN	• ANN stands for an artificial neuron network (ANN) whose underlying bais includes the structure and functions of biological neural networks. This computational model is affected by the information flow through the network since the changes in a neural network depends on that input or output. • Where there are complicated relationships between inputs and outputs or when patterns are established, ANNscan is used as nonlinear statistical data modeling tools.	• Requires less formal statistical restrictions, able to model complex nonlinear relationships, able to train multiple algorithms.	• Big computation burden tends to overfit.	• Huang et al. (2017) • Alama et al. (2016) • Hasan et al. (2019)
Regression	• Regression is used to estimate the relationships between a dependent variable and one or more independent variables.	• Linear • All specifics summarized in one matrix • Logistic regression • Makes no assumptions about distributions of classes in feature space • Easily extended to multiple classes • Natural probabilistic view of class predictions • Quick to train • Resistant to overfitting	• Linear • Doesn't tell us about a particular parameter • Mixes up internal and external parameter • More unknowns than the true degree of freedom • Logistic regression • Linear decision boundary	• Ateeq et al. (2019) • Tekeste et al. (2018) • Chauhan et al. (2018) • Hasan et al. (2019)

Table 6. Potential DL methods for IoT systems

Methods	Working principle	Advantages	Disadvantages	Application in IoT based ERP/ methods reference
Convolutional Neural Networks (CNN)	• CNNs are mainly used to reduce the data parameters in dispersed interactions, to share parameters, and to represent the covariances, thereby reducing inter-layer connections to lower values than those found in ANNs. • CNNs have high computational cost. Therefore, running them on resource-limited devices to support board security systems is challenging.	• CNNs are robust, supervised DL methods that are highly competitive. • The scalability of CNNs has increased with their new features, and their training time complexity has improved compared to ANNs. • Reduces large data.	• CNNs have high computational cost. Therefore, running them on devices with limited resources to support board security systems is challenging.	• Khelifi et al. (2018). • Tang et al. (2017). • Li et al. (2018) • Mohammadi et al. (2018) • Carlos et al.(2019)
Recurrent Neural Networks (RNN)	• The main drawback of RNNs is the issue of disappearance or explosion of slopes. • Tough settings	• RNNs integrate a time layer to capture sequential data and then learn multidimensional changes with the recurrent cell hidden unit. • RNNs and their variants perform well in many applications with sequential data. • Online processing • Keeping Record	• The main drawback of RNNs is the disappearance or explosion of slopes. • Tough settings	• Intrusion detection and prevention mechanism. • Khelifi et al. (2018). • Saeed et al. (2016). • Mohammadi et al. (2018)
Deep Autoencoders (AE)	• AE has a code on its hidden *h* layer, which displays the input. An AE neural network has two parts: the encoder function *h* =, (-), and the decoder function, which endeavors to reproduce input 9: (*h*). The encoder gets the input and converts it into an abstraction, commonly referred to as code. Then, the decoder obtains the code originally generated for input representation to reconstruct the original input.	• AEs can be useful for feature extraction. Instead of manual engineered features, AEs can be effectively used in traditional ML to learn representation for feature learning reduction of dimensions without prior data knowledge.	• AEs takes long computational hours. Although they can learn to effectively record training data features if the training data set does not represent the test data set, the AEs may complicate the learning process rather than representing the data set features.	• Smart grid, smart service, smart city// • Mohammadi et al. (2018).
Restricted Boltzmann machines (RBM)	• The G RBMs are deep production models that are developed for unsupervised learning. They are completely non-directional models in which there is no relationship between two nodes in a layer.	• RBMs are deep production models that are developed forunsupervised learning • They are completely non-directional models in which there is no relationship between two nodes in a layer.	• RBMs have high computational cost. Therefore, their implementation of IoT devices has limited resources to support challenging board security systems.	• Mohammadi, M., et al. (2018).
DBN	• The G R DBNs consist of stacked RBMs that perform greedy layer training to perform robust performance in an unsupervised environment	• DBNs are unsupervised learning methods that are trained to display remarkable features with unlabeled data	• RBMs have high computational cost. Therefore, their implementation of IoT devices has limited resources to support challenging board security systems.	• Mohammadi et al. (2018)
Generative adversarial networks (GAN)	• The GAN framework simultaneously teaches two models (i.e., production and discriminative models) through the opposite process. The production model learns the data distribution and produces the data sample, and the discriminative model predicts the probability that a sample originated from the training dataset rather than the production model (i.e., evaluates the case for accuracy).	• DBNs are In GANs, sample generation requires only a single pass through the model, unlike DBNs and RBMs where an unknown number of Markov chain repetition is required	• DB GAN training is unstable and difficult. Learning to generate discrete data using GAN is a difficult task	• Mohammadi et al. (2018)

Reinforcement learning (RL)	• It differs from supervised learning in that labeled input/output pairs need not be presented, and sub-optimal actions need not be explicitly corrected. Instead, the focus is finding a balance between exploration (of uncharted territory) and exploitation (of current knowledge)	• RL solve the complicated problems which remained unsolved by conventional techniques. • RL is used mostly for long term results, which are difficult to fulfill. • It can be considered an ideal model because of its similarity to the learning of human beings. • The errors of the training process can be corrected by this model. • After an error is corrected, it is very unlikely to encounter the same error again. • RL is capable of creating an ideal model for solving a specific problem. • Robots can learn to walk by implementing RL algorithms.	• RL cannot be used as a framework, and this is a useful point in this technique. • States overload caused by too much RL may result in diminishing the results. • RL is not recommended for simple problems. • A lot of data and computations are required for RL. Actually, it is a data-hungry model, and this is what makes this model excellent for video games. When the game is played over and over again, a lot of data are produced. • According to RL, the world is assumed to be Markovian. However, in reality, this is not the case, because according to the Markovian model,a sequence of possible events is explained, and the probability of each event depends only on the state attained in the previous event.	• Khelifi et al. (2018) • Yao et al. (2015) • Mohammadi et al. (2018) • Xiao et al. (2018) • Chowdhury et al. (2019). • Bu and Wang (2019). • Xiao et al. (2018)