The Internet of Things as A Revolution to Enhance the Technology of the Future

[1]Ahmed Hassan Hassan, [2]Abdilahi Liban, [3]Farah H. Zawaideh, [4]Bara'a Al-Kofahi Instructor, [5]Zakarya Mohsen Al-hodiany, [6]Yazeed Al Moaiad, [*7]Yousef A.Baker El-Ebiary

[1]Dr., Ajloun National University, Faculty of Information Technology, Jordan, Ahmed_hassan@anu.edu.jo
[2]Dr., Faculty of Computer and Information Technology, MEDIU, Malaysia abdilahi.liban@hotmail.com
[3]Prof. Dr., Irbid National University, Jordan dr.farahzawaideh@inu.edu.jo
[4]Deanship of Educational Services-Computer science unit, Qassim University, Saudi Arabia Baraakofh@qu.edu.sa
[5]Faculty of Finance and Admin. Sciences, Al-Madinah International University, Malaysia zakaryahodian@gmail.com
[6]Asst. Prof. Dr., Faculty of Computer and Information Technology, MEDIU, Malaysia yazeed.alsayed@mediu.edu.my
[*7]Assoc. Prof. Ts. Dr., Faculty of Informatics and Computing, UniSZA University, Malaysia, [*](Corresponding Author) yousefelebiary@unisza.edu.my
https://orcid.org/0000-0002-4392-8015

Abstract

Internet of things has brought a technological change or advancement in the traditional system way of living into developed high technological ways of living, examples of Internet of things technological advancement or enhancement is mobile banking, smart devices e.g. Androids and IOS, smart transportation, energy-saving, smart city, pollution controls, and others. There are different types of researches been conducted on how to apply the Internet of things ineffective to traditional ways. However, there are still many challenges facing the applications of the Internet of Things (IoT) in the traditional system. This research will explain some issues facings the use of Internet of things in the traditional system, and the solutions. The article discusses different challenges and key issues of IoT, architecture, and important application domains. Also, the article brings into light the existing literature and illustrated their contribution to different aspects of IoT. Moreover, the importance of big data and its analysis with respect to IoT has been discussed. This article would help the readers and researcher to understand the IoT and its applicability to the real world.

Keywords: Internet of Things (IoT), IoT architectures, IoT challenges, and IoT applications.

I. INTRODUCTION:

IoT connect or communicate electronics devices and sensor through the internet in other to facilitate our lives, IoT is becoming important aspects of our lives that can be sensed

everywhere around us. IoT uses smart devices and internet in other to innovative solutions to various challenges and issues related to various businesses, governmental and public/private industries across the world. IoT is an innovation that puts together extensive variety of smart systems, frameworks and intelligent devices and sensors. (Chen et al., 2014) IoT is based on an extension and expansion of Internet-based network, this elaborate the communication from human and human to human and things or things and things. In the IoT paradigm, many objects surrounding us will be connected into networks in one form or another. RF (Radio Frequencing) identification (RFID), sensor technology, and other smart technologies will be embedded into a variety of applications.

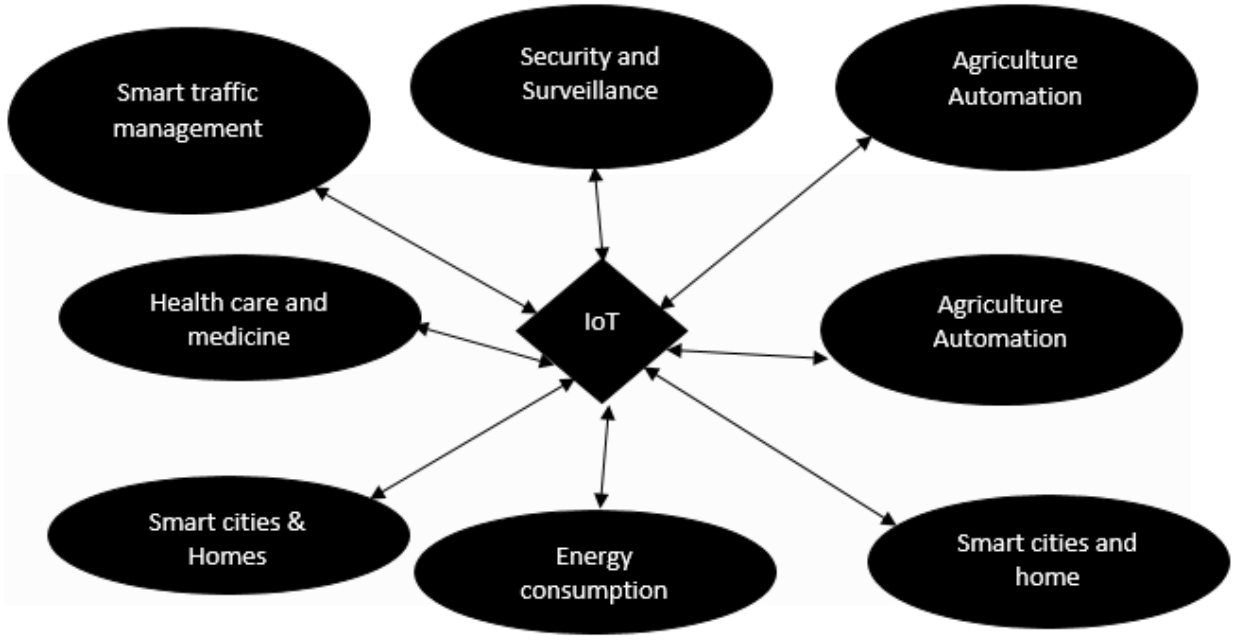
A great transformation can be observed in our daily routine life along with the increasing involvement of IoT devices and technology. One such development of IoT is the concept of Smart Home Systems (SHS) and appliances that consist of internet based devices, automation system for homes and reliable energy management system(Zhou et al., 2017). Besides, another important achievement of IoT is Smart Health Sensing system (SHSS). SHSS incorporates small intelligent equipment and devices to support the health of the human being. These devices can be used both indoors and outdoors to check and monitor the different health issues and fitness level or the amount of calories burned in the fitness center etc. Also, it is being used to monitor the critical health conditions in the hospitals and trauma centers as well. Hence, it has changed the entire scenario of the medical domain by facilitating it with high technology and smart devices(Minoli et al., 2017) . Moreover, IoT developers and researchers are actively involved to uplift the life style of the disabled and senior age group people. IoT has shown a drastic performance in this area and has provided a new direction for the normal life of such people. As these devices and equipment are very cost effective in terms of development cost and easily available within a normal price range, hence most of the people are availing them(Casado-Vara et al., 2019). Thanks to IoT, as they can live a normal life. An important aspect of our dailly life is transportation. IoT brought up some new development to make it more standard, comfortable and reliable. Intelligent technology sensors, drone system are now controlling the traffic at different signalized intersections across major cities. In addition, vehicles are being launched in markets with pre-installed sensing devices that are able to sense the upcoming heavy traffic congestions on the map and may suggest you another route with low traffic congestion(Casado-Vara et al., 2019)(Chen et al., 2014). Therefore, IoT has a lot to serve in various aspects of life and technology. We may conclude that IoT has a lot of scope both in terms of technology enhancement and facilitate the humankind. IoT has also shown its importance and potential in the economic and industrial growth of a developing region. Also, in trade and stock exchange market, it is being considered as a revolutionary step. However, security of data and information is an important concern and highly desirable, which is a major challenging issue to deal with. Internet being a loop hole for security threats and cyber-attacks has opened the various doors for hackers and thus made the data and information insecure. However, IoT is committed to provide the best possible solutions to deal with security issues of data and information. Hence, the most important concern of IoT in trade and economy is security. Therefore, the development of a secure path for collaboration between social networks and privacy concerns is a hot topic in IoT and IoT developers are working hard for this. The remaining part of the article is organized as follows: “Literature survey” section will provide

state of art on important studies that addressed various challenges and issues in IoT. “IoT architecture and technologies” section discussed the IoT functional blocks, architecture in detail. In “Major Key issues and challenges of IoT” section, important key issues and challenges of IoT is discussed. “Major IoT applications” section provides emerging application domains of IoT. In “Importance of big data analytics in IoT” section, the role and importance of big data and its analysis is discussed. Finally, the article concluded in “Conclusions” section.

II. LITERATURE REVIEW

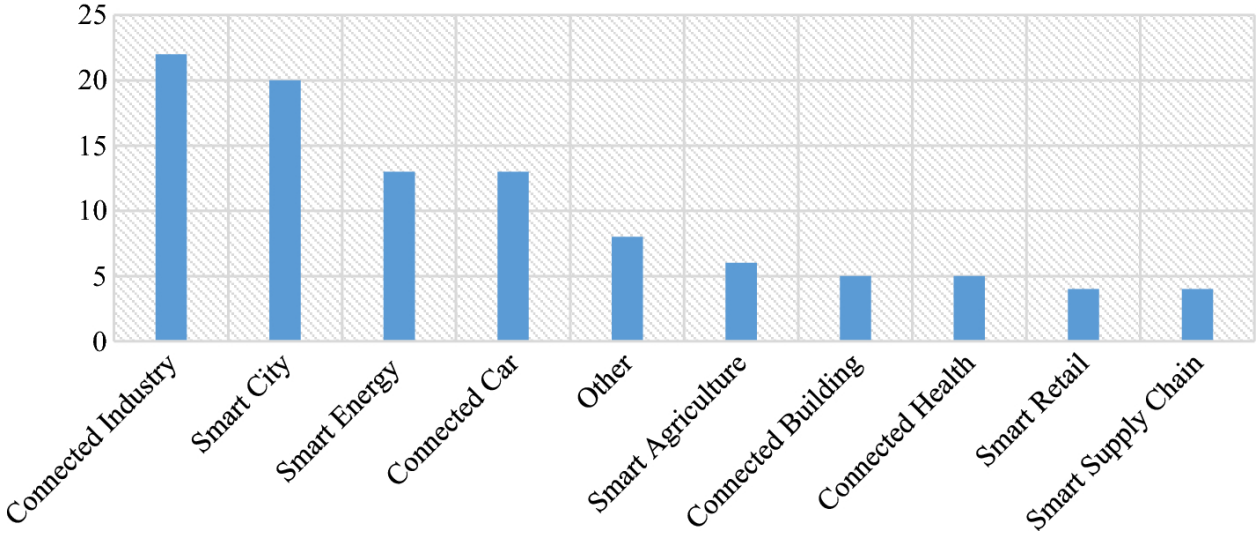
IoT has a many disciplinary vision which provide its benefit to several domains like transportation, industrial, and public/private, medical, environmental. Different researchers have explained the IoT differently with respect to specific interests and aspects. The potential and power of IoT can be seen in several application domains. Figure 1 illustrates few of the application domains of IoTs potentials. Various important IoT projects have taken charge over the market in last few years. Some of the important IoT projects that have captured most of the market are shown in Figure 2. In Figure 2, a global distribution of these IoT projects is shown among American, European and Asia/Pacific region. It can be seen that American continent are contributing more in the health care and smart supply chain projects whereas contribute

Figure 1: IoT application Domains



Various important IoT projects have taken charge over the market in last few years. Some of the important IoT projects that have captured most of the market are shown in Figure 2. In Figure 2, a global distribution of these IoT projects is shown among American, European and Asia/Pacific region. It can be seen that American continent are contributing more in the health care and smart supply chain projects whereas contribution of European continent is more in the smart city projects(Casado-Vara et al., 2019)(*IoT Anal.*, 2016).

Figure 2: Global share of IoT Projects



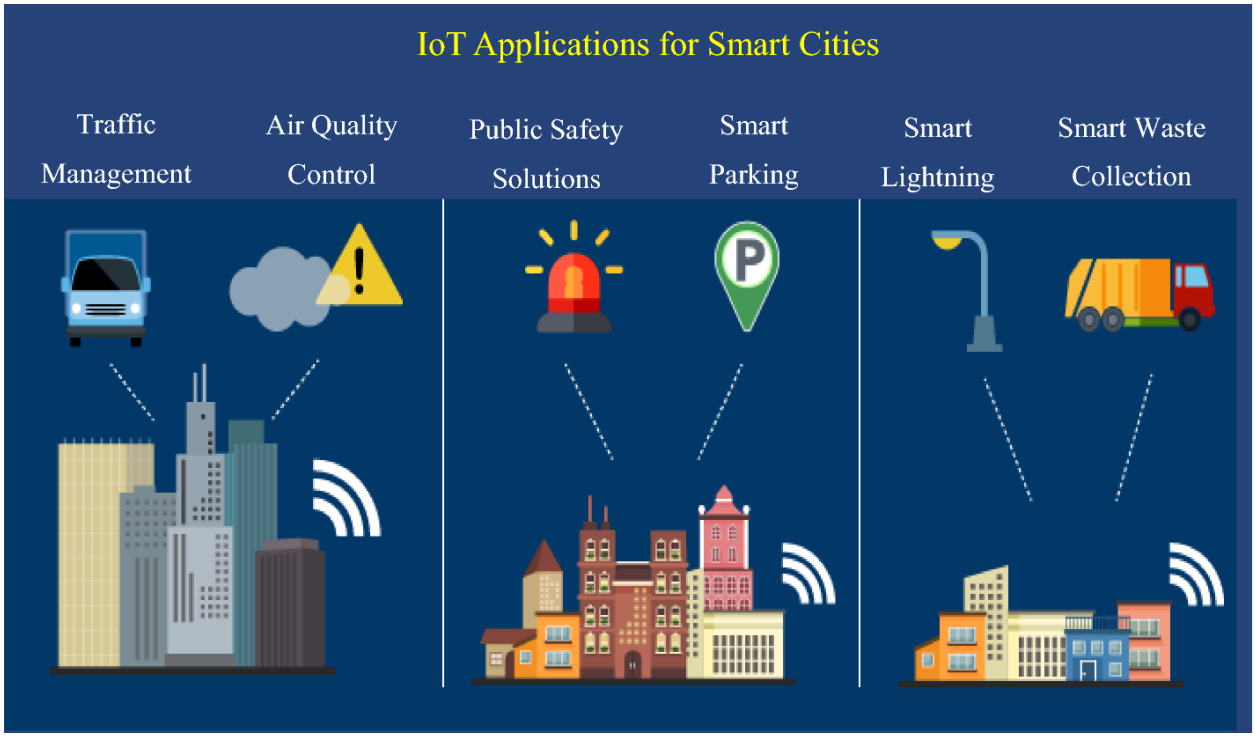
Global distribution of IoT projects among America (USA, South America and Canada), Europe and APAC (Asia and Pacific region)(Casado-Vara et al., 2019)(*IoT Anal.*, 2016)

A lot of research activities(Kumar et al., 2019). The smart home business economy is about to cross the 100 billion dollars by 2022(Zhou et al., 2017). Smart home does not only provide the in-house comfort but also benefits the house owner in cost cutting in several aspects i.e. low energy consumption will result in comparatively lower electricity bill. Besides smart homes, another category that comes within smart city is smart vehicles. Modern cars are equipped with intelligent devices and sensors that control most of the components from the headlights of the car to the engine(Assessed, n.d.). The IoT is committed towards developing a new smart car systems that incorporates wireless communication between car-to-car and car-to-driver to ensure predictive maintenance with comfortable and safe driving experience(Casado-Vara et al., 2019).

Khajenasiri et al.(IoT Anal., 2016) Performed a survey on the IoT solutions for smart energy control to benefit the smart city applications. They stated that at present IoT has been introduced in very few application areas to benefit the people. IoT is very wide and in near future IoT is able to capture almost all the application areas. They mentioned that energy saving is one of the important part of the society and IoT can assist in developing a smart energy control system that will save both energy and money. They described an IoT architecture with respect to smart city concept. The authors also discussed that one of the challenging task in achieving this is the immaturity of IoT hardware and software. They suggested that these issues must be resolved to ensure a reliable, efficient and user friendly IoT system. Alavi et al.(Alavi AH, Jiao P, Buttlar WG, 2018) Addressed the urbanization issue in the cities. People's movement from rural to urban atmosphere resulting in increased population of the cities. However, there is call for the need to provide smart solutions for mobility, energy, healthcare and infrastructure. Smart city is one of the important application areas for IoT developers. It explores several issues such as traffic management, air quality management, public safety solutions, smart parking, smart lightning and smart waste collection Figure 3. they mentioned that IoT is working hard to tackle these challenging issues. The need for improved smart city

infrastructure with growing urbanization has opened the doors for entrepreneurs in the field of smart city technologies. The authors concluded that IoT enabled technology is very important for the development of sustainable smart cities.

Figure 3: IoT Applications for Smart Cities



Another important issue of IoT that requires attention and a lot of research is security and privacy. Weber(Liu et al., 2012) focused on these issues and suggested that a private organization availing IoT must incorporate data authentication, access control, resilience to attacks and client privacy into their business activities that would be an additional advantage. Weber suggested that in order to define global security and privacy issues, IoT developers must take into account the geographical limitations of the different countries. A generic framework needs to be designed to fit the global needs in terms of privacy and security. It is highly recommended to investigate and recognize the issues and challenges in privacy and security before developing the full fledge working IoT framework.

Later, Heer et al.(Weber, 2010) came up with a security issue in IP based IoT system. It is known that internet is essential for the communication among devices that takes place in an IoT system. Therefore, security issues in IP based IoT systems are an important issue. Security architecture should be designed considering the life cycle and capabilities of any object in the IoT system. It includes the involvement of the trusted third party and the security protocols. Architecture security with scalability potential to serve the small-scale and large-scale things in IoT is highly demanded. The study pointed out that IoT gave rise to a new way of communication among several things across the network therefore traditional end to end internet protocol are not able to provide required support to this communication. Therefore, new protocols must be designed considering the translations at the gateways to ensure end-to-

end security. Moreover, all the layers responsible for communication has their own security issues and requirements. Therefore, satisfying the requirements for one particular layers will leave the system into a vulnerable state and security should be ensured for all the layers.

Authentication and access control is another issue in IoT that needs promising solutions to strengthen the security. Liu et al.(Liu et al., 2012) brought up a solution to handle authentication and access control. Authentication is very important to verify the communicating parties to prevent the loss of confidential information. Liu et al.(Minoli et al., 2017)provided an authentication scheme based on Elliptic Curve Cryptosystem and verified it on different security threats i.e. eavesdropping, man-in-the-middle attack, key control and replay attack. They claimed that there proposed schemes are able to provide better authentication and access control in IoT based communication. Later, Kothmayr et al. (Minoli et al., 2017) proposed a two-way authentication scheme based of datagram transport layer security (DTLS) for IoT. The attackers over the internet are always active to steal the secured information. The proposed approach is able to provide message security, integrity, authenticity and confidentiality, memory overhead and end-to-end latency in the IoT based communication network.

Li et al. (Minoli et al., 2017) proposed a dynamic approach for data centric IoT applications with respect to cloud platforms. The need of an appropriate device, software configuration and infrastructure requires efficient solutions to support massive amount of IoT applications that are running on cloud platforms. IoT developers and researchers are actively engaged in developing solutions considering both massive platforms and heterogeneous nature of IoT objects and devices. Olivier et al.(Flauzac et al., 2015) Explained the concept of software defined networking (SDN) based architecture that performs well even if a well-defined architecture is not available. They proposed that SDN based security architecture is more flexible and efficient for IoT.

Luk et al. (Wang et al., 2015) stated that the main task of a secure sensor network (SSN) is to provide data privacy, protection from replay attacks and authentication. They mentioned that although both the SSN services are efficient and reliable, however, ZigBee is comparatively providing higher security but consumes high energy whereas TinySec consumes low energy but not as highly secured as ZigBee.(Abdelhakim et al., 2011) They proposed another architecture MiniSec to support high security and low energy consumption and demonstrated its performance for the Telos platform. Yan et al. (Yan et al., 2014) stated that trust management is an important issue in IoT. Trust management helps people to understand and trust IoT services and applications without worrying about uncertainty issues and risks (Yan et al., 2014). They investigated different issues in trust management and discussed its importance with respect to IoT developers and users.

Noura et al. (Noura, 2019) stated the importance of interoperability in IoT as it allows integration of devices, services from different heterogeneous platforms to provide the efficient and reliable service. Several other studies focused on the importance of interoperability and discussed several challenges that interoperability issue is facing in IoT (Al-Fuqaha et al., 2015)(Palattella, 2015)(Pereira & Aguiar, 2014). Kim et al. (Ray, 2018) addressed the issue of climate change and proposed an IoT based ecological monitoring system. They mentioned that

existing approaches are time consuming and required a lot of human intervention. Also, a routine visit is required to collect the information from the sensors installed at the site under investigation. Also, some information remained missing which leads to not highly accurate analysis. Therefore, IoT based framework is able to solve this problem and can provide high accuracy in analysis and prediction. Later, Wang et al. (Čolaković & Hadžialić, 2018) shows their concern for domestic waste water treatment. They discussed several deficiencies in the process of waste water treatment and dynamic monitoring system and suggested effective solutions based on IoT. They stated that IoT can be very effective in the waste water treatment and process monitoring.

Agriculture is one of the important domain around the world. Agriculture depends on several factors i.e. geographical, ecological etc. Qiu et al. (Flauzac et al., 2015) stated that technology that is being used for ecosystem control is immature with low intelligence level. They mentioned that it could be a good application area for IoT developers and researchers.

Qiu et al. (Fafoutis et al., 2016) proposed an intelligent monitoring platform framework for facility agriculture ecosystem based on IoT that consists of four layer mechanism to manage the agriculture ecosystem. Each layer is responsible for specific task and together the framework is able to achieve a better ecosystem with reduced human intervention.

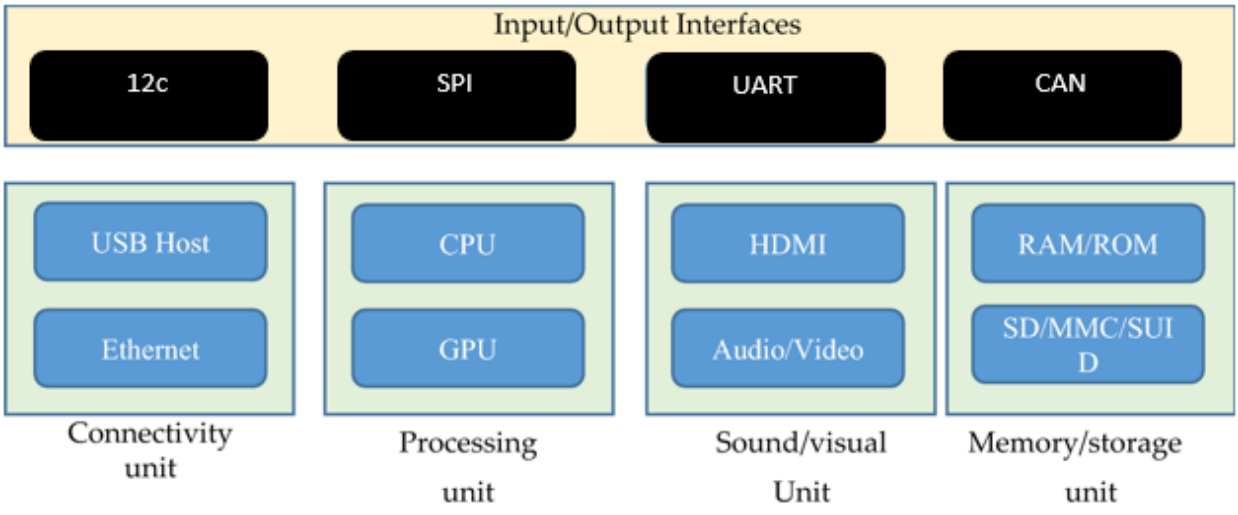
Another important concern around the world is climate change due to global warming. Fang et al. (Sfar et al., 2017) introduced an integrated information system (IIS) that integrates IoT, geo-informatics, cloud computing, global positioning system (GPS), geographical information system (GIS) and e-science in order to provide an effective environmental monitoring and control system. They mentioned that the proposed IIS provides improved data collection, analysis and decision making for climate control. Air pollution is another important concern worldwide. Various tools and techniques are available to air quality measures and control. Cheng et al. (Zhang et al., 2020) proposed AirCloud which is a cloud based air quality and monitoring system. They deployed AirCloud and evaluated its performance using 5 months' data for the continuous duration of 2 months.

Temglit et al. (Technical Solution Working Group (WG2)., 2019) considered Quality of Service (QoS) as an important challenge and a complex task in evaluation and selection of IoT devices, protocols and services. QoS is very important criteria to attract and gain trust of users towards IoT services and devices. They came up with an interesting distributed QoS selection approach. This approach was based on distributed constraint optimization problem and multi-agent paradigm. Further, the approach was evaluated based on several experiments under realistic distributed environments. Another important aspect of IoT is its applicability to the environmental and agriculture standards. Talavera et al. (Technical Solution Working Group (WG2)., 2019) focused in this direction and presented the fundamental efforts of IoT for agro-industrial and environmental aspects in a survey study. They mentioned that the efforts of IoT in these areas are noticeable. IoT is strengthening the current technology and benefiting the farmers and society. Jara et al. (Tzafestas, 2018) discussed the importance of IoT based monitoring of patients health. They suggested that IoT devices and sensors with the help of internet can assist health monitoring of patients.

III. IOT ARCHITECTURE AND TECHNOLOGIES

The IoT architecture consists of five important layers that defines all the functionalities of IoT systems. These layers are perception layer, network layer, middleware layer, application layer, business layer. At the bottom of IoT architecture, perception layer exists that consists of physical devices i.e. sensors, RFID chips, barcodes etc. and other physical objects connected in IoT network. These devices collects information in order to deliver it to the network layer. Network layer works as a transmission medium to deliver the information from perception layer to the information processing system. This transmission of information may use any wired/wireless medium along with 3G/4G, Wi-Fi, Bluetooth etc. Next level layer is known as middleware layer. The main task of this layer is to process the information received from the network layer and make decisions based on the results achieved from ubiquitous computing. Next, this processed information is used by application layer for global device management. On the top of the architecture, there is a business layer which control the overall IoT system, its applications and services. The business layer visualizes the information and statistics received from the application layer and further used this knowledge to plan future targets and strategies. Furthermore, the IoT architectures can be modified according to the need and application domain (Minoli et al., 2017). Besides layered framework, IoT system consists of several functional blocks that supports various IoT activities such as sensing mechanism, authentication and identification, control and management (Carrascal et al., 2020). Figure 4 illustrates such functional blocks of IoT architecture.

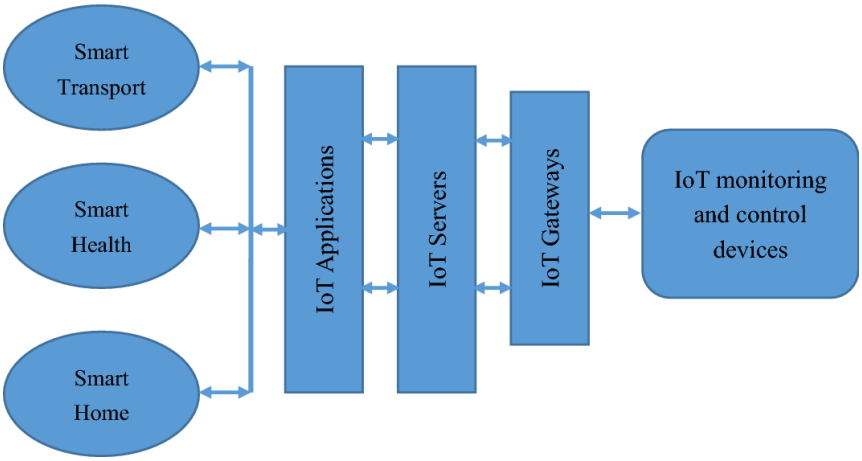
Figure 4: I/O IoT Infrastructure



There are several important functional blocks responsible for I/O operations, connectivity issues, processing, and audio/video monitoring and storage management. All these functional block together incorporates an efficient IoT system which are important for optimum performance. Although, there are several reference architectures proposed with the technical specifications, but these are still far from the standard architecture that is suitable for global IoT. Therefore, a suitable architecture is still needs to be designed that could satisfy the global IoT needs. The generic working structure of IoT system is shown in Figure 5. Figure 5 shows a dependency of IoT on particular application parameters. IoT gateways have an important role

in IoT communication as it allows connectivity between IoT servers and IoT devices related to several applications.

Figure 5: IoT Application Parameters



Scalability, modularity, interoperability and openness are the key design issues for an efficient IoT architecture in a heterogeneous environment. The IoT architecture must be designed with an objective to fulfil the requirements of cross domain interactions, multi-system integration with the potential of simple and scalable management functionalities, big data analytics and storage, and user friendly applications. Also, the architecture should be able to scale up the functionality and add some intelligence and automation among the IoT devices in the system.

Moreover, increasing amount of massive data being generated through the communication between IoT sensors and devices is a new challenge. Therefore, an efficient architecture is required to deal with massive amount of streaming data in IoT system. Two popular IoT system architectures are cloud and fog/edge computing that supports with the handling, monitoring and analysis of huge amount of data in IoT systems. Therefore, a modern IoT architecture can be defined as a 4 stage architecture.

Figure 6: IoT Architecture

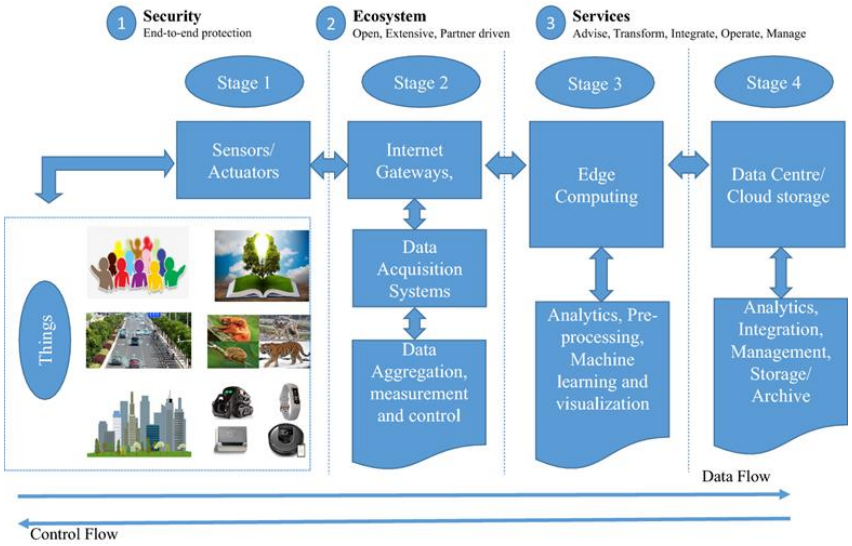


Figure 6, In stage 1 of the architecture, sensors and actuators plays an important role. Real world is comprised of environment, humans, animals, electronic gadgets, smart vehicles, and buildings etc. Sensors detect the signals and data flow from these real world entities and transforms into data which could further be used for analysis. Moreover, actuators are able to intervene the reality i.e. to control the temperature of the room, to slow down the vehicle speed, to turn off the music and light etc. Therefore, stage 1 assist in collecting data from real world which could be useful for further analysis. Stage 2 is responsible to collaborate with sensors and actuators along with gateways and data acquisition systems. In this stage, massive amount of data generated in stage 1 is aggregated and optimized in a structured way suitable for processing. Once the massive amount of data is aggregated and structured then it is ready to be passed to stage 3 which is edge computing. Edge computing can be defined as an open architecture in distributed fashion which allows use of IoT technologies and massive computing power from different locations worldwide. It is very powerful approach for streaming data processing and thus suitable for IoT systems. In stage 3, edge computing technologies deals with massive amount of data and provides various functionalities such as visualization, integration of data from other sources, analysis using machine learning methods etc. The last stage comprises of several important activities such as in depth processing and analysis, sending feedback to improve the precision and accuracy of the entire system. Everything at this stage will be performed on cloud server or data centre. Big data framework such as Hadoop and Spark may be utilized to handle this large streaming data and machine learning approaches can be used to develop better prediction models which could help in a more accurate and reliable IoT system to meet the demand of present time.

IV. MAJOR KEY ISSUES AND CHALLENGES OF IOT

The involvement of IoT based systems in all aspects of human lives and various technologies involved in data transfer between embedded devices made it complex and gave rise to several issues and challenges. These issues are also a challenge for the IoT developers in the advanced smart tech society. As technology is growing, challenges and need for advanced IoT system is also growing. Therefore, IoT developers need to think of new issues arising and should provide solutions for them.

A. Security and privacy issues

One of the most important and challenging issues in the IoT is the security and privacy due to several threats, cyber-attacks, risks and vulnerabilities. The issues that give rise to device level privacy are insufficient authorization and authentication, insecure software, firmware, web interface and poor transport layer encryption. Security and privacy issues are very important parameters to develop confidence in IoT Systems with respect to various aspects. Security mechanisms must be embedded at every layer of IoT architecture to prevent security threats and attacks. Several protocols are developed and efficiently deployed on every layer of communication channel to ensure the security and privacy in IoT based systems. Secure Socket Layer (SSL) and Datagram Transport Layer Security (DTLS) are one of the cryptographic protocols that are implemented between transport and application layer to provide security solutions in various IoT systems. However, some IoT applications require different methods to

ensure the security in communication between IoT devices. Besides this, if communication takes place using wireless technologies within the IoT system, it becomes more vulnerable to security risks. Therefore, certain methods should be deployed to detect malicious actions and for self-healing or recovery. Privacy on the other hand is another important concern which allows users to feel secure and comfortable while using IoT solutions. Therefore, it is required to maintain the authorization and authentication over a secure network to establish the communication between trusted parties. Another issue is the different privacy policies for different objects communicating within the IoT system. Therefore, each object should be able to verify the privacy policies of other objects in IoT system before transmitting the data.

B. Interoperability/standard issues

Interoperability is the feasibility to exchange the information among different IoT devices and systems. This exchange of information does not rely on the deployed software and hardware. The interoperability issue arises due to the heterogeneous nature of different technology and solutions used for IoT development. The four interoperability levels are technical, semantic, syntactic and organizational. Various functionalities are being provided by IoT systems to improve the interoperability that ensures communication between different objects in a heterogeneous environment. Additionally, it is possible to merge different IoT platforms based on their functionalities to provide various solutions for IoT users. Considering interoperability an important issue, researchers approved several solutions that are also known as interoperability handling approaches. These solutions could be adapters/gateways based, virtual networks/overlay based, service oriented architecture based etc. Although interoperability handling approaches ease some pressure on IoT systems but there are still certain challenges remain with interoperability that could be a scope for future studies.

C. Ethics, law and regulatory rights

Another issue for IoT developers is the ethics, law and regulatory rights. There are certain rules and regulations to maintain the standard, moral values and to prevent the people from violating them. Ethics and law are very similar term with the only difference is that ethics are standards that people believes and laws are certain restrictions decided by the government. However, both ethics and laws are designed to maintain the standard, quality and prevent people from illegal use. With the development of IoT, several real life problems are solved but it has also given rise to critical ethical and legal challenges. Data security, privacy protection, trust and safety, data usability is some of those challenges. It has also been observed that majority of IoT users are supporting government norms and regulations with respect to data protection, privacy and safety due to the lack of trust in IoT devices. Therefore, this issue must be taken into consideration to maintain and improve the trust among people for the use of IoT devices and systems.

D. Scalability, availability and reliability

A system is scalable when new features are possible to be added, equipment's and devices without degrading its performance. The main issue with IoT is to support a large number of devices with different memory, processing, storage power and bandwidth (Fafoutis et al., 2016).

Another important issue that must be taken into consideration is the availability. Scalability and availability both should be deployed together in the layered framework of IoT. A great example of scalability is cloud based IoT systems which provide sufficient support to scale the IoT network by adding up new devices, storage and processing power as required.

In addition, the global distributed IoT network gives rise to a new research paradigm to develop a smooth IoT framework that satisfy global needs (Tzafestas, 2018). One of the challenges is the adequate availability of resources to the authentic objects regardless of their location and time of the requirement. In a distributed fashion, several small IoT networks are timely attached to the global IoT platforms to utilize their resources and services. Therefore, availability is an important concern (Zhang et al., 2020). Due to the use of different data transmission channels i.e. satellite communication, some services and availability of resources may be interrupted. Therefore, an independent and reliable data transmission channel is required for uninterrupted availability of resources and services.

Table 1: Major IoT applications

	Location sensing and sharing	Environmental servicing	Remote controlling	Ad hoc network	Secure communication
Emerging economy		√	√		√
Smart City	√		√		
Transportation and vehicle				√	
Agriculture and industry automation	√		√		√
Environmental	√				
Health-care	√	√			

V. FINDINGS

A. Emerging economy, environmental and health-care

IoT is can provide an advance emerging public and financial benefits and development to the society for the benefits of people. This includes a wide range of public facilities i.e. economic development, water quality maintenance, well-being, industrialization etc. Overall, IoT is working hard to accomplish the social, health and economic goals of United Nations advancement step. Environmental sustainability is another important concern. IoT developers must be concerned about environmental impact of the IoT systems and devices to overcome the negative impact. Energy consumption by IoT devices is one of the challenges related to environmental impact.it requires lot of Energy consumption high rate due to internet enabled services and edge cutting devices. This area needs research for the development of high quality materials in order to create new IoT devices with lower energy consumption rate. Also, green

technologies can be adopted to create efficient energy efficient devices for future use. It is not only environmental friendly but also advantageous for human health. Researchers and engineers are engaged in developing highly efficient IoT devices to monitor several health issues such as diabetes, obesity or depression. Several issues related to environment, energy and healthcare are considered by several studies.

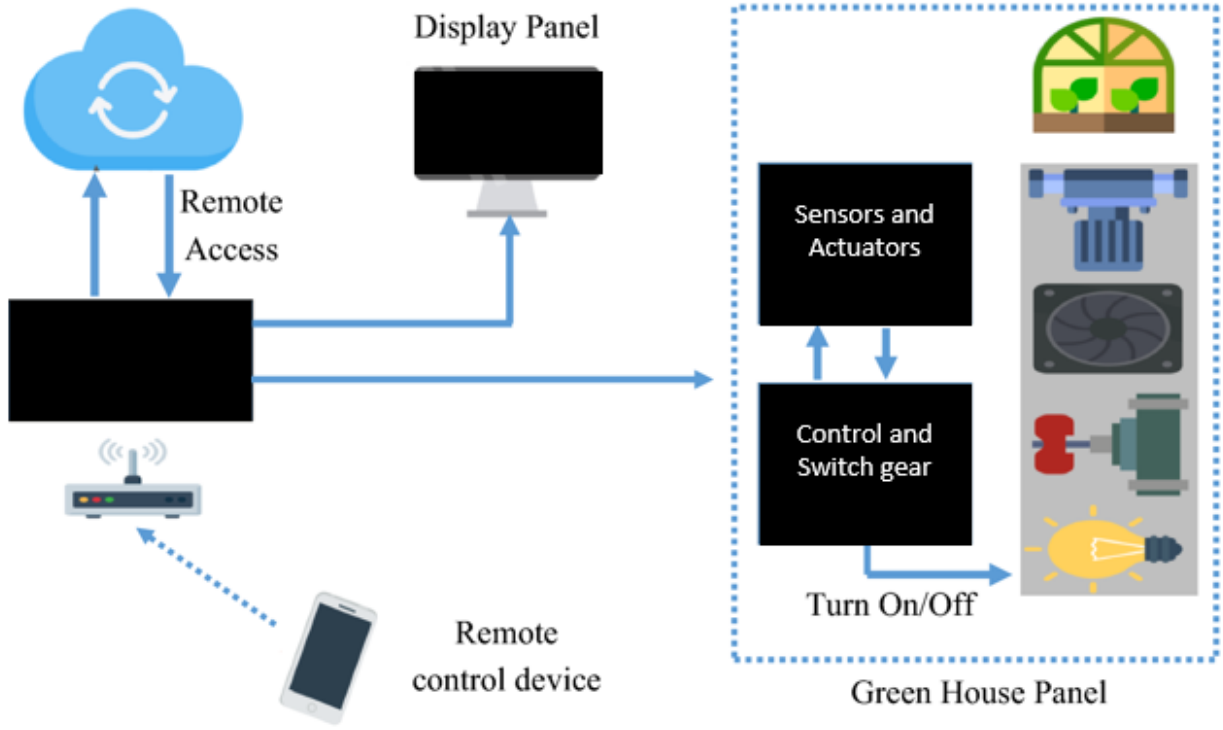
B. Smart city, transport and vehicles

IoT is transforming the traditional civil structure of the society into high tech structure with the concept of smart city, smart home and smart vehicles and transport. Rapid improvements are being done with the help of supporting technologies such as machine learning, natural language processing to understand the need and use of technology at home. Various technologies such as cloud server technology, wireless sensor networks that must be used with IoT servers to provide an efficient smart city. Another important issue is to think about environmental aspect of smart city. Therefore, energy efficient technologies and Green technologies should also be considered for the design and planning of smart city infrastructure. Further, smart devices which are being incorporated into newly launched vehicles are able to detect traffic congestions on the road and thus can suggest an optimum alternate route to the driver. This can help to lower down the congestion in the city. Furthermore, smart devices with optimum cost should be designed to be incorporated in all range vehicles to monitor the activity of engine. IoT is also very effective in maintaining the vehicle's health. Self-driving cars have the potential to communicate with other self-driving vehicles by the means of intelligent sensors. This would make the traffic flow smoother than human-driven cars who used to drive in a stop and go manner. This procedure will take time to be implemented all over the world. Till the time, IoT devices can help by sensing traffic congestion ahead and can take appropriate actions. Therefore, a transport manufacturing company should incorporate IoT devices into their manufactured vehicles to provide its advantage to the society.

C. Agriculture and industry automation

The world's growing population is estimated to reach approximate 10 billion by 2050. Agriculture plays an important role in our lives. In order to feed such a massive population, we need to advance the current agriculture approaches. Therefore, there is a need to combine agriculture with technology so that the production can be improved in an efficient way. Greenhouse technology is one of the possible approaches in this direction. It provides a way to control the environmental parameters in order to improve the production. However, manual control of this technology is less effective, need manual efforts and cost, and results in energy loss and less production. With the advancement of IoT, smart devices and sensors makes it easier to control the climate inside the chamber and monitor the process which results in energy saving and improved production Figure 7. Automation of industries is another advantage of IoT. IoT has been providing game changing solutions for factory digitalization, inventory management, quality control, logistics and supply chain optimization and management.

Figure 7: IoT Automation System



D. Importance of big data analytics in IoT

An IoT system comprises of a huge number of devices and sensors that communicates with each other. With the extensive growth and expansion of IoT network, the number of these sensors and devices are increasing rapidly(Sfar et al., 2017). These devices communicate with each other and transfer a massive amount of data over internet. This data is very huge and streaming every second and thus qualified to be called as big data. Continuous expansion of IoT based networks gives rise to complex issue such as management and collection of data, storage and processing and analytics. IoT big data framework for smart buildings is very useful to deal with several issues of smart buildings such as managing oxygen level, to measure the smoke/hazardous gases and luminosity. Such framework is capable to collect the data from the sensors installed in the buildings and performs data analytics for decision making. Moreover, industrial production can be improved using an IoT based cyber physical system that is equipped with an information analysis and knowledge acquisition techniques. Traffic congestion is an important issue with smart cities. The real time traffic information can be collected through IoT devices and sensors installed in traffic signals and this information can be analyzed in an IoT based traffic management system. In healthcare analysis, the IoT sensors used with patients generate a lot of information about the health condition of patients every second. This large amount of information needs to be integrated at one database and must be processed in real time to take quick decision with high accuracy and big data technology is the best solution for this job. IoT along with big data analytics can also help to transform the traditional approaches used in manufacturing industries into the modern one. The sensing devices generates information which can be analyzed using big data approaches and may help in various decision making tasks. Furthermore, use of cloud computing and analytics can

benefit the energy development and conservation with reduced cost and customer satisfaction. IoT devices generate a huge amount of streaming data which needs to be stored effectively and needs further analysis for decision making in real time. Deep learning is very effective to deal with such a large information and can provide results with high accuracy. Therefore, IoT, Big data analytics and Deep learning together is very important to develop a high tech society.

VI. CONCLUSIONS

Recent advancements in IoT have drawn attention of researchers and developers worldwide. IoT developers and researchers are working together to extend the technology on large scale and to benefit the society to the highest possible level. However, improvements are possible only if we consider the various issues and shortcomings in the present technical approaches. In this survey article, we presented several issues and challenges that IoT developer must take into account to develop an improved model. Also, important application areas of IoT is also discussed where IoT developers and researchers are engaged. As IoT is not only providing services but also generates a huge amount of data. Hence, the importance of big data analytics is also discussed which can provide accurate decisions that could be utilized to develop an improved IoT system.

References

1. Abdelhakim, M., Lightfoot, L. E., & Li, T. (2011). Reliable data fusion in wireless sensor networks under Byzantine attacks. Proceedings - IEEE Military Communications Conference MILCOM, 810–815. https://doi.org/10.1109/MILCOM.2011.6127777
2. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys and Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095.
3. Somanshu Choudhary, Keshav Kumar, Bishwajeet Pandey, Teshu Pankhuri, Kamini Simi Bajaj, Yousef A. Baker El-Ebiary. "Soil Moisture and Environmental Temperature and Humidity Sensor-Based Data Breaches in IoT Enable Irrigation System Design using Arduino and FPGA" Vol.6, No.2, pp. 1-12, July 2020, GJET, DOI: 10.21058/gjet.2020.62001,
4. Alavi AH, Jiao P, Buttlar WG, L. N. (2018). Internet of things-enabled smart cities: state-of-the-art and future trends. Measurement. ; 129:589–606. https://books.google.com.my/books?id=4TbPDwAAQBAJ&pg=PA589&lpg=PA589&dq=Alavi+AH,+Jiao+P,+Buttlar+WG,+Lajnef+N.+Internet+of+things-enabled+smart+cities:+state-of-the-art+and+future+trends.+Measurement.+2018;129:589–606&source=bl&ots=Wv7Sgp95lT&sig=ACfU3U1
5. Assessed. (n.d.). Internet of Things. https://www.ti.com/technologies/internet-of-things/overview.html
6. Carrascal, D., Rojas, E., Alvarez-Horcajo, J., Lopez-Pajares, D., & Martínez-Yelmo, I. (2020). Analysis of P4 and XDP for IoT Programmability in 6G and Beyond. IoT, 1(2), 605–622. https://doi.org/10.3390/iot1020031
7. Casado-Vara, R., Novais, P., Gil, A. B., Prieto, J., & Corchado, J. M. (2019). Distributed Continuous-Time Fault Estimation Control for Multiple Devices in IoT Networks. IEEE Access, 7, 11972–11984. https://doi.org/10.1109/ACCESS.2019.2892905
8. Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with China Perspective. IEEE Internet of Things Journal, 1(4), 349–359. https://doi.org/10.1109/JIOT.2014.2337336
9. Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks, 144(October), 17–39. https://doi.org/10.1016/j.comnet.2018.07.017

10. Fafoutis, X., Tsimbalo, E., Mellios, E., Hilton, G., Piechocki, R., & Craddock, I. (2016). A residential maintenance-free long-term activity monitoring system for healthcare applications. Eurasip Journal on Wireless Communications and Networking, 2016(1), 1–20. https://doi.org/10.1186/s13638-016-0534-3
11. Flauzac, O., Gonzalez, C., & Nolot, F. (2015). New security architecture for IoT network. Procedia Computer Science, 52(1), 1028–1033. https://doi.org/10.1016/j.procs.2015.05.099
12. IoT Analytics. (2016). IoT Analytics. https://iot-analytics.com/top-10-iot-project-application-areas-q3-2016/
13. Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6(1). https://doi.org/10.1186/s40537-019-0268-2
14. Liu, J., Xiao, Y., & Chen, C. L. P. (2012). Authentication and access control in the Internet of things. Proceedings - 32nd IEEE International Conference on Distributed Computing Systems Workshops, ICDCSW 2012, 588–592. https://doi.org/10.1109/ICDCSW.2012.23
15. Minoli, D., Sohraby, K., & Kouns, J. (2017). IoT security (IoTSec) considerations, requirements, and architectures. 2017 14th IEEE Annual Consumer Communications and Networking Conference, CCNC 2017, 1006–1007. https://doi.org/10.1109/CCNC.2017.7983271
16. Noura, M. (2019). Interoperability in Internet of Things : Taxonomies and Open Challenges. 796–809.
17. Palattella, M. R. (2015). Internet of Things in the 5G Era : Enabling Technologies and Business Models Internet of Things (IoT) definition. IEEE Journal on Selected Areas in Communications, December 2015, 1–9. https://orbilu.uni.lu/bitstream/10993/24796/1/main_jsac.pdf
18. Pereira, C., & Aguiar, A. (2014). Towards efficient mobile M2M communications: Survey and open challenges. Sensors (Switzerland), 14(10), 19582–19608. https://doi.org/10.3390/s141019582
19. Ray, P. P. (2018). A survey on Internet of Things architectures. Journal of King Saud University - Computer and Information Sciences, 30(3), 291–319. https://doi.org/10.1016/j.jksuci.2016.10.003
20. Sfar, A. R., Chtourou, Z., & Challal, Y. (2017). A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges. 2017 International Conference on Smart, Monitored and Controlled Cities, SM2C 2017, 101–105. https://doi.org/10.1109/SM2C.2017.8071828
21. Technical Solution Working Group (WG2). (2019). Driving Data to the Edge: The Challenge of Traffic Distribution. Aecc. https://aecc.org/wp-content/uploads/2019/09/AECC_WG2_TR_v1.0.2.pdf
22. Belal Alifan, Mokhairi Makhtar, Yousef El-Ebiary. “Propose Model for Consumers’ Perceptions and Acceptance of e-Health Systems and Services in Jordan” Vol. 68, Editor’s Issues, Oct. 2020, pp. 1-10, IJETT, doi: 10.14445/22315381/CATI3P201.
23. Tzafestas, S. (2018). Ethics and Law in the Internet of Things World. Smart Cities, 1(1), 98–120. https://doi.org/10.3390/smartcities1010006.
24. Hazem M Bani Abdoh, Syarilla Iryani A. Saany, Hamid H. Jebur, Yousef El-Ebiary. “The Effect of PESTLE Factors on E-Government Adoption in Jordan: A Conceptual Model” Vol. 68, Editor’s Issues, Oct. 2020, pp. 19-23, IJETT, doi: 10.14445/22315381/CATI3P203.
25. Wang, J. Y., Cao, Y., Yu, G. P., & Yuan, M. Z. (2015). Research on application of IOT in domestic waste treatment and disposal. Proceedings of the World Congress on Intelligent Control and Automation (WCICA), 2015-March(March), 4742–4745. https://doi.org/10.1109/WCICA.2014.7053515
26. Weber, R. H. (2010). Internet of Things - New security and privacy challenges. Computer Law and Security Review, 26(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008
27. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). Journal of Network and Computer Applications A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42, 120–134. https://doi.org/10.1016/j.jnca.2014.01.014
28. Zhang, W. E., Sheng, Q. Z., Mahmood, A., Tran, D. H., Zaib, M., Hamad, S. A., Aljubairy, A., Alhazmi, A. A. F., Sagar, S., & Ma, C. (2020). The 10 Research Topics in the Internet of Things. Proceedings - 2020 IEEE 6th International Conference on Collaboration and Internet Computing, CIC 2020, 34–43. https://doi.org/10.1109/CIC50333.2020.00015
29. 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. https://doi.org/10.1109/MCOM.2017.1600363CM