Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 38-47 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

CONCEPTS, APPLICATIONS, AND CHALLENGES OF THE INTERNET OF THINGS

Nauryzbek Amangeldiyev, Master student, Mechanical engineering faculty, Hungarian University of Agriculture and Life Sciences.

Patrick Siegfried, Professor, Doctor, Doctor, MBA, Logistics & Supply Chain Management, ISM International School of Management GmbH – Gemeinnützige Gesellschaft, Guest Professor at the Hungarian University of Agriculture and Life Sciences.

ABSTRACT: The main aim of the study is to give the reader the basic meaning of an "Internet of Things" itself, evaluate its main concepts, types, trends, and areas of application, as well as challenges.

The study is a basic and fresh literature review from general sources and researches on the topic that has been done recently by the scientific community. Qualitative and quantitative methods of data collecting have been used. As a result, this paper can offer new interpretations, theoretical approaches, or other ideas. Mendeley referencing application was used to cite and give credits to the authors of a raw material used in this study.

This term paper will give an excellent understanding to other researchers who are trying to build basic concepts within the topic, or to those who wish to begin their researches on "IoT" furthermore and will provide effective and accumulation knowledge. Also, can be useful as a raw material to the introductory courses regarding "IoT".

KEYWORDS – *IoT; Internet of things; IoT security; IoT vision; Internet of nano-Things; IoT architecture; Layers of IoT; Smart Planet; Smart Home; Smart Transport; Smart Healthcare; Smart Transportation; Smart City; Smart Energy Grid; Internet of People; IoP; IoE; Internet of Everything*

INTRODUCTION

The Internet of Things – (IoT) is a new concept in which the Internet is evolving from the unification of computers and people to the unification of (smart) objects/things (Gubbi et al., 2013). With the continuous advancement of Internet of Things technologies, potential innovations are "crashing down" on us, growing to a global computing network where everything and everyone will be connected via the Internet. IoT is constantly evolving and is a hot topic for research at the moment. The usual form of the Internet is moving into its modified and integrated version. The number of devices using Internet services is growing every day and connecting them all with wires or wireless technology will give us a powerful source of information at our fingertips. The concept of empowering interactions between smart machines is cutting-edge technology. But the technologies that make up the Internet of Things are nothing new.

IoT is an approach to connecting information received from various sources on any virtual platform or existing Internet infrastructure. The concept "Internet of Things" appeared in 1982, when a modified soda machine was connected to the Internet and was able to report the presence of drinks in it and their temperature. Later, in 1991, Mark Weiser was the first to give a modern assessment of the Internet of Things.

Moreover, in 1999, Bill Joy gave a hint about the connection between devices in his Internet taxonomy (Said & Masud, 2013). In the same year, Kevin Ashton proposed the term "Internet of Things" for connected devices. The basic idea of IoT is to provide the possibility of autonomous exchange of useful information. These devices are equipped with the latest technology such as radio frequency identification (RFID) and wireless sensor networks (WSN) and in the ability to get the opportunity to make independent decisions depending on which automated execution is being performed.

CONCEPT

In 2005, the International Telecommunications Union (ITU), heralds an era of pervasive networks, the main hallmark of which is connectivity networks among themselves. The main concept of the Internet of Things is the

environment in which things can obey control, and data about things can be processed to perform the desired task by training the devices (Alam et al., 2020). Practical implementation of IoT is well demonstrated in Twine, compact and low-power hardware that works melting with real-time network software and allowing make this concept a reality (Arndt, 2017).

However, different people and organizations have differing concepts of the Internet of Things. In connection with the rapid development of packet-switched networks, and above all the Internet, in the early 2000s, the global telecommunications community first developed, and then it began to implement a new paradigm for the development of communications – next-generation networks (NGN). NGN technologies have already passed the evolutionary path of development from flexible switches (Softswitch) to multimedia communication subsystems IMS (IP Multimedia Subsystem) and long-term wireless networks evolution of LTE. It has always been assumed that the main users of NGN networks will be people and, therefore, the maximum number of subscribers in such networks will always be limited by the population of planet Earth (Singh et al., 2020). However, in recent years, RFID (Radio Frequency Identification) methods, WSN (Wireless Sensor Network), short-range communications NFC (Near Field Communication) and M2M (Machine-to-Machine) communications have received significant development. integrating with the Internet, they make it possible to provide a simple connection between various technical devices ("things"), the number of which can be huge.

Thus, there is an evolutionary transition from the "Internet of people" to the "Internet of things" (Miranda et al., 2015). In the general case, the Internet of Things is understood as a set of various devices, sensors, devices connected into a network through any available communication channels using various protocols of interaction with each other and a single protocol for accessing the global network. The Internet is currently used in the role of the global network for the Internet of Things. The common protocol is IP.

ARCHITECTURE

Cisco believes that in 2020 there will be more than 50 billion connected objects with a population of 7 billion people (Cisco, 2015). The existing Internet architecture with its TCP/IP protocols cannot cope with such a large network as IoT. Therefore, there is a need for a new open architecture that can send reports on the safety, quality, and class of data transmission services with quality of services (QoS) provided, while at the same time supporting existing network applications using open protocols. The Internet of Things cannot be implemented without proper security guarantees. Therefore, data protection and privacy are key tasks for IoT.

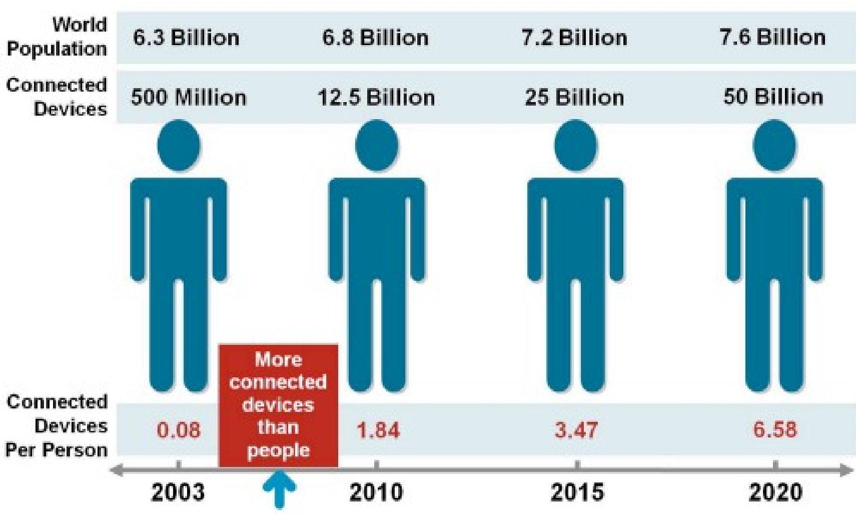

FIGURE 1
TIMELINE OF CHANGES IN THE NUMBER OF PEOPLE AND OBJECTS, CONNECTED TO THE INTERNET (Evans, 2011)

For further development, IoT offers several multi-level architectures. The Internet of Things conceptually belongs to the next generation of networks, so its architecture is in many ways similar to the well-known four-layer of NGN architecture (Singh et al., 2020). IoT consists of a set of various information and communication technologies that ensure the functioning of the Internet of Things, and its architecture shows how these technologies are connected. The architecture includes four functional layers (Figure 2) described below.

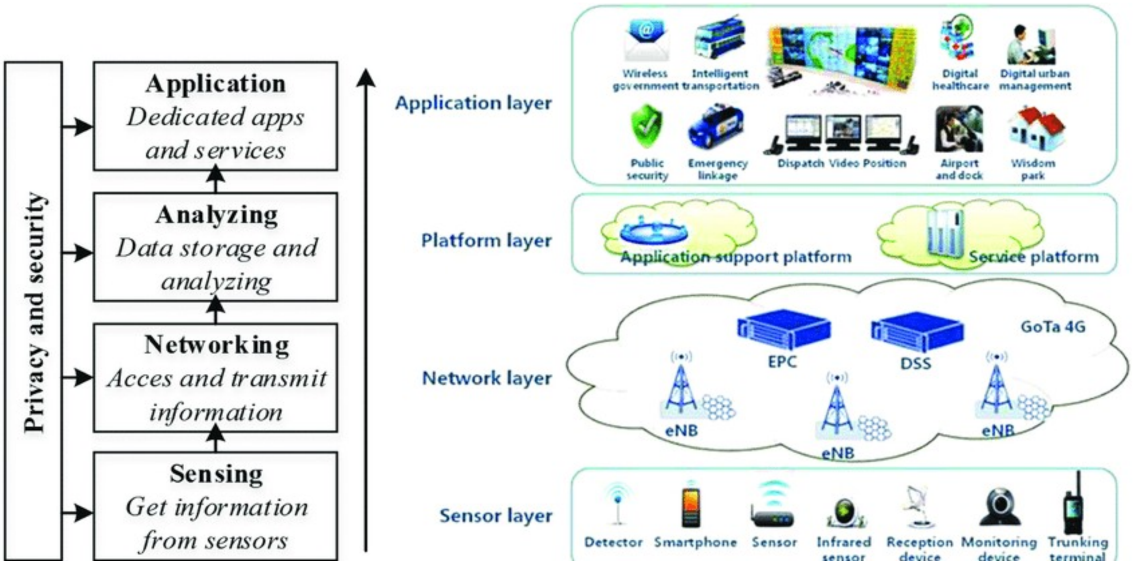

FIGURE 2
FOUR FUNCTIONAL LAYERS OF IOT (RAD ET AL., 2015)

The level of sensors and sensor networks. The lowest level of the IoT architecture consists of smart objects integrated with sensors (sensors). Sensors realize the connection of the physical and virtual (digital) worlds, providing the collection and processing of information in real-time. Miniaturization, which led to a reduction in the physical size of hardware sensors, made it possible to integrate them directly into objects of the physical world. There are various types of sensors for specific purposes, for example, for measuring temperature, pressure, speed, location, etc. Sensors can have small memory, making it possible to record several measurement results. The sensor can measure the physical parameters of the monitored object/phenomenon and convert them into a signal that can be received by the corresponding device. Sensors are classified according to their purpose, for example, environmental sensors, body sensors, home appliance sensors, vehicle sensors, etc. (Ratnaparkhi et al., 2020). Most sensors require a connection to a sensor aggregator (gateway), which can be implemented using a Local Area Network (LAN) such as Ethernet and Wi-Fi or a Personal Area Network (PAN) such as ZigBee, Bluetooth, and Ultra-Wide Band Wireless (UWB). For sensors that do not require a connection to the aggregator, their connection to servers/applications can be provided using wide-area wireless WANs such as GSM, GPRS and LTE. Sensors, which are characterized by low power consumption and low data rates, form the well-known Wireless Sensor Networks (WSN). WSNs are gaining in popularity as they can contain many more battery-enabled sensors and cover large areas.

Gateway and network layer. The large amount of data generated at the first layer of the IoT by multiple miniature sensors requires a reliable and high-performance wired or wireless network infrastructure as a transport medium. Existing networks communications using different protocols can be used to support M2M machine-to-machine communications and their applications. To implement a wide range of services and applications in the IoT, it is necessary to ensure that many networks of different technologies and access protocols work together in a heterogeneous configuration. These networks must provide the required values of the quality of information transmission, and above all in terms of delay, bandwidth, and security. This level consists of converged network infrastructure, which is created by integrating heterogeneous networks into a single network platform. Converged Abstract Network Layer in IoT allows multiple users to share resources on the same network independently and jointly through appropriate gateways without compromising privacy, security, or performance (Divarci & Urhan, 2018).

Service level (Analyzing). The service level contains a set of information services designed to automate technological and business operations in the IoT: support for operational and business activities (OSS / BSS, Operation Support System / Business Support System), various analytical processing of information (statistical, data mining and text mining, predictive analytics, etc.), data storage, information security, business rule management (BRM), business process management (BPM), etc.

Application layer. At the fourth level of the IoT architecture, there are various types of applications for the respective industrial sectors and spheres of activity (energy, transport, trade, medicine, education, etc.). Applications can be "vertical" when they are specific to a particular industry, as well as "horizontal" (eg, fleet management, asset tracking, etc.) that can be used in different sectors of the economy.

INTERNET OF “NANO” THINGS

Nanotechnology has led to the development of miniature devices, the sizes of which range from one to several hundred nanometers. At this level, nano-machines consist of nano components and represent themselves as separate functional units capable of performing simple measuring, regulating, or controlling operations. Coordination and information exchange between nano-devices allow the formation of so-called nano-networks. In the case of connecting nano-devices to existing networks and a new network paradigm is emerging on the Internet, called the “Internet of Nano-things”. The interaction of nano-devices with existing networks and the Internet require the development of new network architectures (Nayyar et al., 2017). Figure 3 shows the architecture of the Internet of nano-things in two different implementations – a network on the human body for monitoring health indicators and sending them to a medical centre, and a modern office network connecting many different devices.

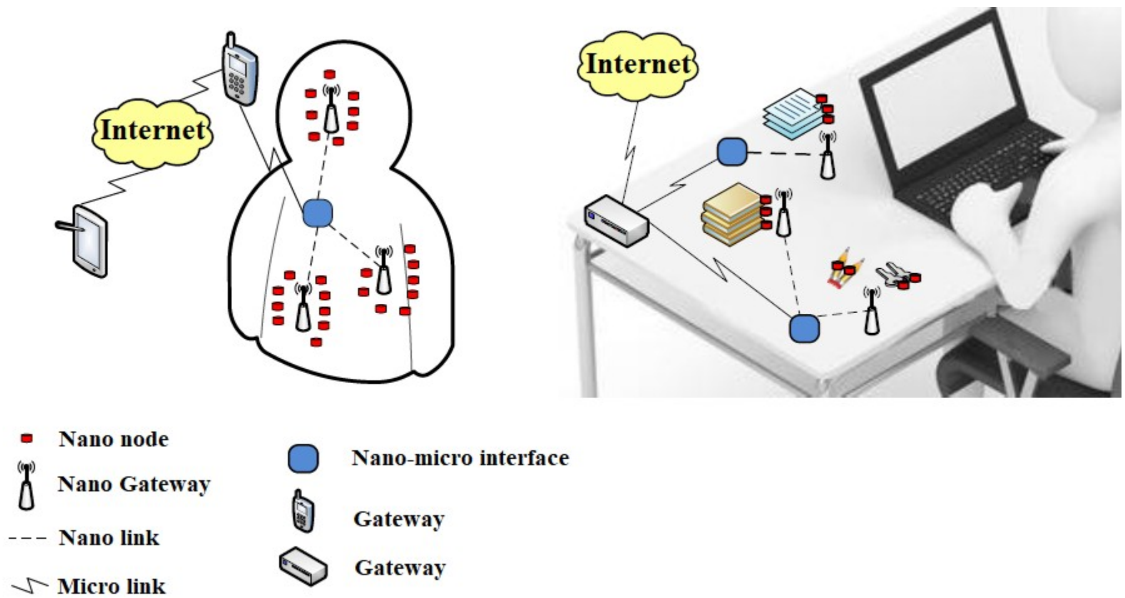

FIGURE 3
INTERNET OF NANO-THINGS EXAMPLE ARCHITECTURE

The network on the human body consists of nano-sensors and nano actuators that can send information through an external gateway to a medical facility. In this case, at the nano-level, molecules, proteins, DNA, organic substances, and basic components of cells. Thus, biological nano-sensors and nano-actuators provide an interface between the human biological environment and electronic nano-devices that can be used in a new network paradigm - the Internet of Nano-Things. The intraoffice network connects many even the smallest devices with nano-transceivers that provide an Internet connection. As a result of this interaction, the user can track the status and location of things, without any effort and time. When developing new miniature devices, the most advanced energy-saving technologies can be used to obtain mechanical, electromagnetic, and other types of energy from the environment.

Regardless of the field of application, the main components of the architecture of the Internet of nano-things are:

1. Nano-nodes are miniature and simplest nano-devices. They allow us to perform the simplest calculations, have limited memory and a limited signal transmission range. Examples of nano-nodes can be biological nano-sensors on or inside the human body or nano-devices embedded in everyday things around us – books, watches, keys, etc.
2. Nano-gateways - these nano-devices have relatively high performance compared to nano-nodes and perform the function of collecting information from nano-nodes. In addition, nano-gateways can control the behaviour of nano-nodes by executing simple commands (on/off, sleep mode, transmit data, etc.).

3. Nano-micro interfaces are devices that collect information from nano-gateways and transmit it to external networks. These devices include both nano-communication technologies and traditional technologies for transmitting information to existing networks.
4. Gateway – this device monitors the entire nano-network via the Internet. For example, in the case of a network with sensors on the human body, this function can be performed by a mobile phone that transmits information about the necessary indicators to a medical institution.

DIRECTIONS OF THE PRACTICAL APPLICATION OF IOT

Based on the Internet of Things, all kinds of "smart" applications can be implemented in various spheres of human activity and life (Figure 4):

- "Smart Planet" - a person can literally "keep his finger on the pulse" of the planet: respond promptly to omissions in household planning, pollution, and other environmental problems, and therefore effectively manage non-renewable resources. Individual large-scale projects in the direction of creating a "smart" planet, a kind of "Intranet of things", have been developing vigorously in recent years. Thus, the US National Aeronautics and Space Administration (NASA), with the support of Cisco, is creating a system for global data collection about the Earth - the "Skin of the Planet" (Planetary skin) (NASA, Cisco Partnering for Climate Change Monitoring Platform, n.d.). It is planned to develop an online platform for collecting and analyzing data on the environmental situation coming from space, air, sea, and ground sensors scattered throughout our planet. This data will be made available to the general public, Governments, and commercial organizations. They will make it possible to measure, report and verify environmental data in near real-time, to recognize global climate changes promptly and adapt to them (NASA, Cisco Partnership on Climate Change Monitoring Platform | The Network, n.d.). The development of the platform began with a series of pilot projects, including the Rainforest Skin project (lit. - "the skin of the tropical jungle"), during which the process of destruction of tropical forests on a global scale will be investigated. Individual large-scale projects in the direction of creating a "smart" planet, a kind of "Intranet of things", have been developing vigorously in recent years. Thus, the US National Aeronautics and Space Administration (NASA), with the support of Cisco, is creating a system for global data collection about the Earth - the "Skin of the Planet" (Planetary skin) (*How NASA, Cisco, And A Tricked-Out Planetary Skin Could Make The World*, n.d.). It is planned to develop an online platform for collecting and analyzing data on the environmental situation coming from space, air, sea, and ground sensors scattered throughout our planet. This data will be made available to the general public, Governments, and commercial organizations. They will make it possible to measure, report and verify environmental data in near real-time, to recognize global climate changes promptly and adapt to them. The development of the platform began with a series of pilot projects, including the Rainforest Skin project (lit. - "the skin of the tropical jungle"), during which the process of destruction of tropical forests on a global scale will be investigated (Juan Carlos Castilla-Rubio & Simon Willis, 2009).
- "Smart City – urban infrastructure and related municipal services, such as education, healthcare, public safety, housing, and communal services, will become more connected and efficient. In recent years, information systems have been intensively created in cities to automate certain areas of urban life: urban environment security, transport, energy and housing, healthcare, education, public and municipal administration, etc. The principles and technologies of IoT make it possible to create a fully connected integrated solution necessary for the functioning of the urban and accessible to all residents of the city, employees of city services, officials, and managers of different levels (Javed et al., 2020). The most effective U-systems (connected based on the Internet of Things) are municipal, transport, parking services, as well as the service for combating street and domestic crime. These are, in fact, the key problems of urban life that can be solved based on a unified monitoring and control system. So, in a Korean city, Yeonpyeong New Town effectively operates a U-system in the field of trade in the form of a portal with information about shops, cafes, etc., as well as a system for monitoring the location of children, designed for parents.
- "Smart home" - the system will recognize specific situations occurring in the house and respond to them accordingly, which will provide residents with safety, comfort, and resource conservation. "Smart home" is

designed for the most comfortable life of people through the use of modern high-tech tools. The principle of operation of the smart home system is to automate everything that a residential building consists of lighting, air conditioning, security system, electricity, heating, water supply and sanitation, and so on. The main subsystems of the "smart home" include climate control, lighting, multimedia (audio and video), security systems, communications, and others (Al-Mutawa & Eassa, 2020).

- "Smart energy" – reliable and high-quality transmission of electrical energy from the source to the receiver will be provided at the right time and in the required amount. Currently, the most developed application of IoT technologies is "Smart Grids" in the energy sector (Abir et al., 2021). The operation of such a network is based on the fact that the supplier and the consumer get an objective picture of the use of energy resources through monitoring all sections of the network and, as a result, get the opportunity for operational management. In case of accidents, such networks can automatically identify problem areas and, within a short time, direct electricity through backup circuits, restoring the power supply. For consumers, "smart" networks mean opportunities for flexible regulation of electricity consumption, both in "manual" and automatic mode.
- "Smart transport – moving passengers from one point of space to another will become more convenient, faster and safer. Intelligent transport systems (ITS) based on IoT technologies allow for automatic interaction between infrastructure facilities and a vehicle V2I (Vehicle to Infrastructure) or between different vehicles V2V (Vehicle to Vehicle) (Dey et al., 2016). V2V systems exchange data wirelessly between machines at a distance of up to several hundred meters. V2I systems carry out the exchange between the vehicle and traffic control centres, road operators and service companies. The data transmitted by infrastructure objects are integrated into a common system and transmitted to nearby vehicles. Technologies of both groups can significantly increase the safety and efficiency of transport (Gupta et al., 2020).
- "Smart Medicine– - doctors and patients will be able to get remote access to expensive medical equipment or electronic medical history anywhere, a remote health monitoring system will be implemented, the delivery of medicines to patients will be automated, and much more. "Smart medicine" based on the Internet of Things is usually implemented in practice in the form of human health monitoring systems using a variety of biosensors and sensors and remote medical care systems. Possible applications of sensor network-based monitoring systems in medicine:

  1. Monitoring of the physiological state of a person: physiological data collected by sensory networks can be stored for a long period and can be used for medical research. Installed network nodes can also track the movements of the elderly, disabled people and, for example, prevent falls. These nodes are small and provide the patient with greater freedom of movement, while at the same time allowing doctors to identify the symptoms of the disease in advance. In addition, they contribute to providing a more comfortable life for patients in comparison with hospital treatment.

  2. Monitoring of doctors and patients in the hospital: each patient has a small and light network node. Each node has its specific task. For example, one can monitor the heart rate, while the other takes blood pressure readings. Doctors may also have such a node; it will allow other doctors to find them in the hospital.

  3. Monitoring of medicines in hospitals: sensor nodes can be attached to medicines, then the chances of issuing the wrong medicine can be minimized. So, patients will have nodes that determine their allergies and the necessary medications. (Farahani et al., 2018)

Computerized systems have shown that they can help minimize the side effects of erroneous drug administration. One of the stages of improving modern medicine is the personalization of data and increasing communication between doctors. Easy access to the medical history, allows you to prescribe timely effective treatment. The management of medical records may gradually move to the network. "Cloud" solutions are used to store large amounts of information on the Internet. Thanks to the Internet, doctors from different clinics get access to patient data. Electronic medical records make it possible to find out about the patient's health promptly, prescribe effective treatment. Linking the equipment of a medical institution into a single network will allow you to receive the necessary data on portable devices of doctors, which receive information about the patient: what medications are prescribed, test results, etc. The introduction of Internet technologies saves time for the patient and the doctor. There is no need to get to the polyclinic, it is only necessary to turn on the computer and you can contact the medical institution. Video calls make it possible not only to make a survey but also to make a general examination, which is often enough for a general idea of human health. If you still need to see a doctor, then you can also make an appointment via the Internet. Pressure measuring devices, scales and other portable equipment are equipped with wireless transmitters that allow you to immediately transfer data to a computer and keep records of your health. A "smart clothing" is being developed that collects data on a person's condition: heart rate, body temperature, respiratory rate. Chips are sewn into such smart clothes at the development stage, which not only carries out measurements but also allows transmitting data to a mobile phone (Espinosa et al., 2021).

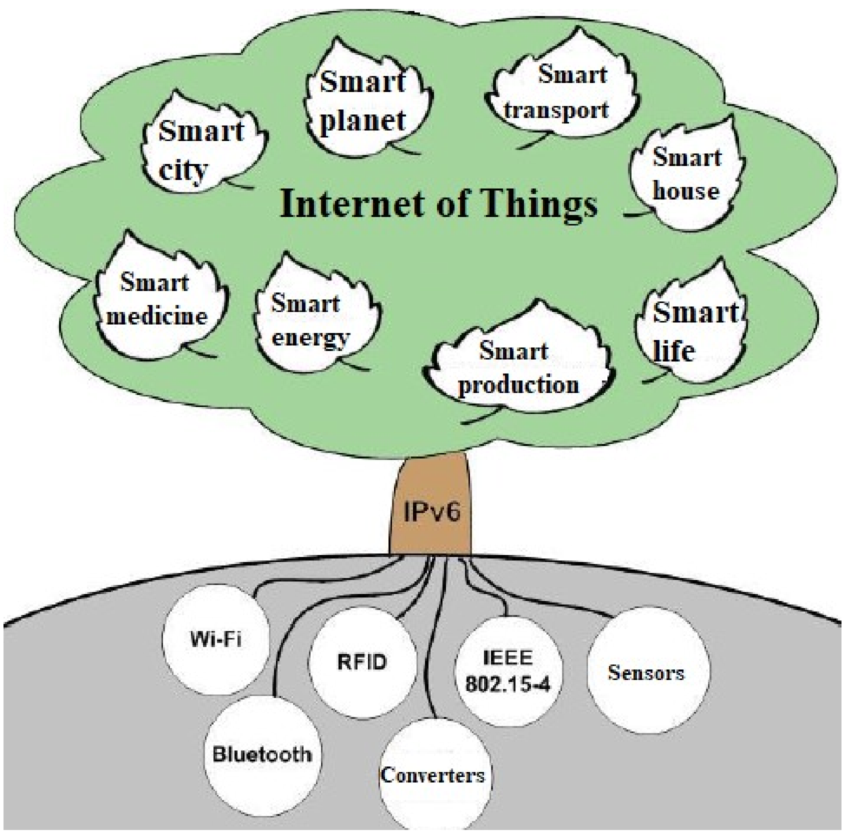

FIGURE 4
SMART APPLICATIONS ON THE BASE OF THE INTERNET OF THINGS

You have many acknowledgements. Please put the sponsor acknowledgements in this section; do not use a footnote on the first page.

PROBLEMS OF IOT IMPLEMENTATION

The widespread adoption of the Internet of Things is hindered by complex technical and organizational problems, in particular, related to standardization. There are no uniform standards for the Internet of Things yet, which makes it difficult to integrate the solutions offered on the market and largely constrains the emergence of new ones. The vagueness of the formulations of the concept of the Internet of Things and a large number of regulators and their regulations hinder global implementation the most.

The factors slowing down the development of the Internet of Things include the difficulties of the transition of the existing Internet to the new, 6th version of the IP network protocol, primarily the need for large financial costs on the part of telecommunications operators and service providers to modernize their network equipment. *If technological platforms for the Internet of Things have already been practically created, then, for example, legal and psychological ones are still only in the formative stage, as well as problems of interaction between users, data, devices.* One of the problems is data protection in such global networks. There is also a serious problem associated with the invasion of privacy by the Internet of Things. The ability to track the location of people and their property raises the question of who will have this information at their disposal.

Who will be responsible for storing the information collected by "smart things"? To whom and under what conditions will this information be provided? Is it possible to collect it without a person's consent? All these questions remain open for now. Also, for the full functioning of such a network, the autonomy of all "things" is necessary, i.e., sensors must learn to receive energy from the environment, and not work from batteries, as is happening now. In addition, with the advent of the Internet of Things, there will be a need to change generally accepted and proven business processes and strategies, which can lead to significant financial costs and risks (Kao et al., 2019). The main drivers and problems of implementing the Internet of Things are given in Table 1. However, all of these disadvantages are not significant compared to what opportunities the Internet of Things can provide for humanity. Therefore, sooner or later humanity will inevitably make extensive use of IoT technologies. But to successfully implement these technologies, we need to know them. As a present future scope, it is highly recommended to develop italicized ideas and answer the questions.

TABLE I
DRIVERS AND BARRIERS OF IOT (INGLE & GHODE, 2017; PADYAB ET AL., 2020)

Drivers	Barriers
The rapid development of info-communication technologies	The need to adopt common standards
Fashion for smartphones, tablets, and other mobile devices	Slow transition to IPv6
Logistics and supply management	Risk of closure of private networks
Improving the safety and convenience of vehicles	Incompatibility of several components
The need to preserve the environment and reduce energy costs	The problem of personal data protection and security
Development of the sphere of control over counterfeit products and protection against theft	Relatively high cost of implementation
State support and actions of innovators	

CONCLUSION

The Internet of People (IoP) that exists today brings real benefits to many individuals, companies, and entire countries. The web drives economic growth through e-commerce and accelerates business innovation by fostering collaboration. The Internet has helped improve the education system by democratizing access to information resources (Siegfried, 2015, Siegfried, 2014). Almost all of our daily life (work, education, leisure, entertainment and much more) is already unthinkable without the Web. But today we are entering an era when the new Internet of Things (IoT) can radically improve the lives of everyone on our planet - to help solve climate problems, heal serious diseases, improve business processes, and make every day of our lives happier.

Cisco predicts that we will inevitably move to the Internet of Everything (IoE), where all sorts of inanimate objects will begin to take into account the context and take advantage of wider computing resources and sensory capabilities. Cisco defines IoE as connecting people, processes, data, and things that add value to network connections to unprecedented levels. IoE transforms information into concrete actions that create new opportunities, enhance the user experience, and create an enabling environment for the development of countries, companies, and users.

This definition highlights an important aspect of IoE that distinguishes it from IoT - the so-called "network effect". As we connect to the Internet, more and more new items, of people and data, the power of the Internet (as a network of networks) grows, according to Matcalfe's law, in proportion to the square of the number of users. This means that the value of the network is a higher arithmetic sum of its components. Because of this, the possibilities of the Universal Internet IoE should become truly limitless, and **this is currently the biggest challenge for IoT, to become IoE**.

REFERENCES

1. Abir, S. M. A. A., Anwar, A., Choi, J., & Kayes, A. S. M. (2021). Iot-enabled smart energy grid: Applications and challenges. *IEEE Access*, *9*, 50961–50981. https://doi.org/10.1109/ACCESS.2021.3067331

2. Alam, M., Shakil, K. A., & Khan, S. (2020). Internet of things (IoT): Concepts and applications. In the *Internet of Things (IoT): Concepts and Applications*. Springer International Publishing. https://doi.org/10.1007/978-3-030-37468-6
3. Al-Mutawa, R. F., & Eassa, F. A. (2020). A smart home system based on the internet of things. *International Journal of Advanced Computer Science and Applications*, *2*, 260–267. https://doi.org/10.14569/ijacsa.2020.0110234
4. Arndt, R. Z. (2017). Bridging the healthcare gap through digital coaching, online resources. *Modern Healthcare*, *47*(49), 30. https://search.ebscohost.com/login.aspx?direct=true&AuthType=athens,cookie,ip,uid&db=cin20&AN=126780107&site=ehost-live
5. Cisco. (2015). The Internet of Things : Reduce Security Risks with Automated Policies. *Cisco White Paper*.
6. Dey, K. C., Rayamajhi, A., Chowdhury, M., Bhavsar, P., & Martin, J. (2016). Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network - Performance evaluation. *Transportation Research Part C: Emerging Technologies*, *68*, 168–184. https://doi.org/10.1016/j.trc.2016.03.008
7. Divarci, S., & Urhan, O. (2018). Secure gateway for network layer safety in IoT systems. *26th IEEE Signal Processing and Communications Applications Conference, SIU 2018*. https://doi.org/10.1109/SIU.2018.8404785
8. Espinosa, Á. V., López, J. L., Mata, F. M., & Estevez, M. E. (2021). Application of iot in healthcare: Keys to implementation of the sustainable development goals. In *Sensors* (Vol. 21, Issue 7). MDPI AG. https://doi.org/10.3390/s21072330
9. Evans, D. (2011). How the Next Evolution of the Internet Is Changing Everything. *CISCO White Paper*, *April*.
10. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems*, *78*, 659–676. https://doi.org/10.1016/j.future.2017.04.036
11. 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. https://doi.org/10.1016/j.future.2013.01.010
12. Gupta, M., Benson, J., Patwa, F., & Sandhu, R. (2020). Secure V2V and V2I Communication in Intelligent Transportation using Cloudlets. *IEEE Transactions on Services Computing*, 1–1. https://doi.org/10.1109/tsc.2020.3025993
13. *How NASA, Cisco, And A Tricked-Out Planetary Skin Could Make The World*. (n.d.). Retrieved November 16, 2021, from https://www.fastcompany.com/3024393/how-nasa-cisco-and-a-tricked-out-planetary-skin-could-make-the-world-a-sa
14. Ingle, A. P., & Ghode, S. (2017). Internet of Things (IoT): Vision, Review, Drivers of IoT, Sensors Nodes, Communication Technologies and Architecture. *International Journal of Advances in Computer and Electronics Engineering*, *2*(8), 1–7.
15. Javed, A., Kubler, S., Malhi, A., Nurminen, A., Robert, J., & Framling, K. (2020). BIoTope: Building an IoT Open Innovation Ecosystem for Smart Cities. *IEEE Access*, *8*, 224318–224342. https://doi.org/10.1109/ACCESS.2020.3041326
16. Juan Carlos Castilla-Rubio, & Simon Willis. (2009, March). *Planetary Skin*. A Cisco Internet Business Solutions Group (IBSG). https://docplayer.net/16234718-Planetary-skin-authors-juan-carlos-castilla-rubio-simon-willis-cisco-internet-business-solutions-group-ibsg.html

17. Kao, Y. S., Nawata, K., & Huang, C. Y. (2019). Evaluating the performance of systemic innovation problems of the IoT in manufacturing industries by novel MCDM methods. *Sustainability (Switzerland)*, *11*(18). https://doi.org/10.3390/su11184970

18. Miranda, J., Mäkitalo, N., Garcia-Alonso, J., Berrocal, J., Mikkonen, T., Canal, C., & Murillo, J. M. (2015). From the Internet of Things to the Internet of People. In *IEEE Internet Computing* (Vol. 19, Issue 2, pp. 40–47). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/MIC.2015.24

19. *NASA, Cisco Partnering For Climate Change Monitoring Platform*. (n.d.). Retrieved November 16, 2021, from https://www.nasa.gov/home/hqnews/2009/mar/HQ_09046_NASA_Cisco.html

20. *NASA, Cisco Partnership on Climate Change Monitoring Platform | The Network*. (n.d.). Retrieved November 16, 2021, from https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=4802571

21. Nayyar, A., Puri, V., & Le, D.-N. (2017). Internet of Nano Things (IoNT): Next Evolutionary Step in Nanotechnology. *Nanoscience and Nanotechnology*, *7*(1), 4–8. http://article.sapub.org/10.5923.j.nn.20170701.02.html

22. Padyab, A., Habibipour, A., Rizk, A., & Ståhlbröst, A. (2020). Adoption barriers of IoT in large scale pilots. *Information (Switzerland)*, *11*(1). https://doi.org/10.3390/info11010023

23. Rad, C.-R., Hancu, O., Takacs, I.-A., & Olteanu, G. (2015). Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture. *Agriculture and Agricultural Science Procedia*, *6*. https://doi.org/10.1016/j.aaspro.2015.08.041

24. Ratnaparkhi, S., Khan, S., Arya, C., Khapre, S., Singh, P., Diwakar, M., & Shankar, A. (2020). Smart agriculture sensors in IOT: A review. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2020.11.138

25. Said, O., & Masud, M. (2013). Towards internet of things: Survey and future vision. *International Journal of Computer Networks*, *5*(1), 1–17. http://www.cscjournals.org/csc/manuscript/Journals/IJCN/volume5/Issue1/IJCN-265.pdf

26. Siegfried, P. (2015) Die Unternehmenserfolgsfaktoren und deren kausale Zusammen-hänge, Zeitschrift Ideen- und Innovationsmanagement, Deutsches Institut für Betriebs-wirtschaft GmbH/Erich Schmidt Verlag, ISSN 2198-3143, S. 131-137. https://doi.org/10.37307/j.2198-3151.2015.04.04

27. Siegfried, P. (2014) Analysis of the service research studies in the German research field, Performance Measurement and Management, Publishing House of Wroclaw University of Economics, ISBN: 978-83-7695-473-8, Band 345, pp. 94-104. DOI: 10.15611/pn.2014.345.09

28. Singh, S., Sheng, Q. Z., Benkhelifa, E., & Lloret, J. (2020). Guest Editorial: Energy Management, Protocols, and Security for the Next-Generation Networks and Internet of Things. In *IEEE Transactions on Industrial Informatics* (Vol. 16, Issue 5). https://doi.org/10.1109/TII.2020.2964591