IOT AS CORE ELEMENT IN ECOSYSTEM

Usmanova Nargiza
D.Sc.,Professor, in Telecommunication technologies department in Tashkent University of Information Technologies named after Muhammad al – Khwarizmi in Tashkent, Uzbekistan,

Yunusova Dilnoza
Master in Telecommunication technologies department in Tashkent University of Information Technologies named after Muhammad al – Khwarizmi in Tashkent, Uzbekistan,
e-mail: 92dilichka@gmail.com

ABSTRACT*: The Internet of Things (IoT) continues to grow and develop rapidly. Internet of things, is considered the driving factor of the 4th industrial revolution. In the present era of advanced technology, IoT makes a vital contribution toward the development of sophisticated knowledge-aware systems for various growing sectors, like healthcare, education, intelligent cities, savvy homes, automized agriculture, etc. Through an IoT ecosystem, core elements and their importance or meaning can be defined.*

Any specialized IoT solution consists of several layers: a communication network, devices, clouds where data is processed, and the platforms themselves that analyze the data. All of them should be available from the same ecosystem

Key words: *IoT ecosystem, Architecture, Cloud computing, Data analytics, Machine learning.*

INTRODUCTION

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction [1].

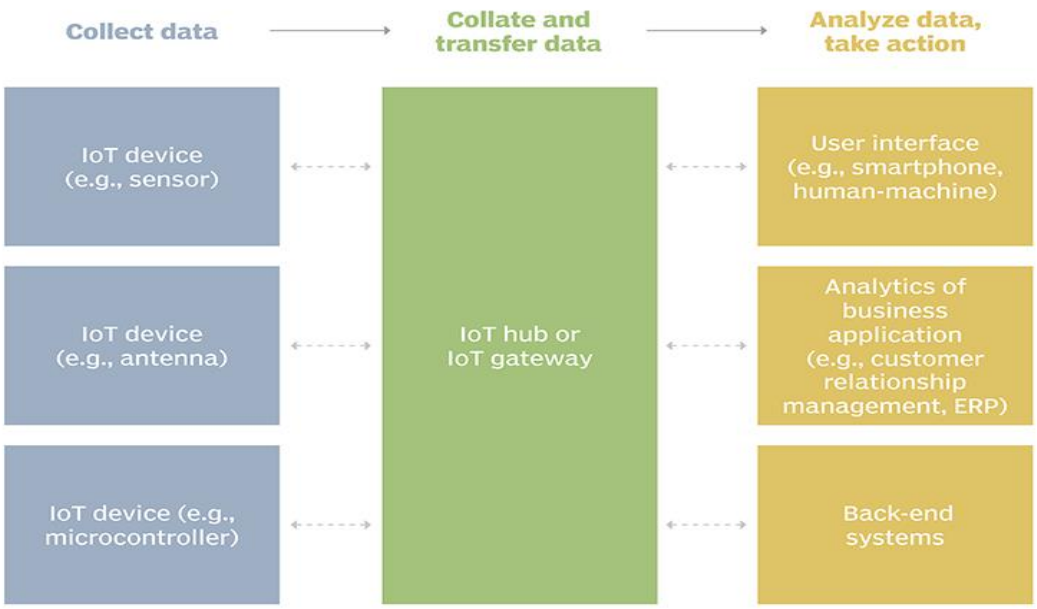
A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business.

METHODS

An IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another [2]. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data (fig. 1.).

Fig1. Example of an IoT system



What are the pros and cons of IoT? Some of the advantages of IoT include the following:

ability to access information from anywhere at any time on any device;

improved communication between connected electronic devices;

transferring data packets over a connected network saving time and money; and

automating tasks helping to improve the quality of a business's services and reducing the need for human intervention.

Some disadvantages of IoT include the following:

As the number of connected devices increases and more information is shared between devices, the potential that a hacker could steal confidential information also increases.

Enterprises may eventually have to deal with massive numbers -- maybe even millions -- of IoT devices, and collecting and managing the data from all those devices will be challenging.

If there's a bug in the system, it's likely that every connected device will become corrupted.

Since there's no international standard of compatibility for IoT, it's difficult for devices from different manufacturers to communicate with each other.

RESULTS

IoT standards and frameworks. There are several emerging IoT standards, including the following [3]:

IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) is an open standard defined by the Internet Engineering Task Force (IETF). The 6LoWPAN standard enables any low-power radio to communicate to the internet, including 804.15.4, Bluetooth Low Energy (BLE) and Z-Wave (for home automation).

ZigBee is a low-power, low-data rate wireless network used mainly in industrial settings. ZigBee is based on the Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 standard. The ZigBee Alliance created Dotdot, the universal language for IoT that enables smart objects to work securely on any network and understand each other.

LiteOS is a Unix-like operating system (OS) for wireless sensor networks. LiteOS supports smartphones, wearables, intelligent manufacturing applications, smart homes and the internet of vehicles (IoV). The OS also serves as a smart device development platform.

OneM2M is a machine-to-machine service layer that can be embedded in software and hardware to connect devices. The global standardization body, OneM2M, was created to develop reusable standards to enable IoT applications across different verticals to communicate.

Data Distribution Service (DDS) was developed by the Object Management Group (OMG) and is an IoT standard for real-time, scalable and high-performance M2M communication.

Advanced Message Queuing Protocol (AMQP) is an open source published standard for asynchronous messaging by wire. AMQP enables encrypted and

interoperable messaging between organizations and applications. The protocol is used in client-server messaging and in IoT device management.

Constrained Application Protocol (CoAP) is a protocol designed by the IETF that specifies how low-power, compute-constrained devices can operate in the internet of things.

Long Range Wide Area Network (LoRaWAN) is a protocol for WANs designed to support huge networks, such as smart cities, with millions of low-power devices.

IoT frameworks include the following:

Amazon Web Services (AWS) IoT is a cloud computing platform for IoT released by Amazon. This framework is designed to enable smart devices to easily connect and securely interact with the AWS cloud and other connected devices.

Arm Mbed IoT is a platform to develop apps for IoT based on Arm microcontrollers. The goal of the Arm Mbed IoT platform is to provide a scalable, connected and secure environment for IoT devices by integrating Mbed tools and services.

Microsoft's Azure IoT Suite is a platform that consists of a set of services that enables users to interact with and receive data from their IoT devices, as well as perform various operations over data, such as multidimensional analysis, transformation and aggregation, and visualize those operations in a way that's suitable for business.

Google's Brillo/Weave is a platform for the rapid implementation of IoT applications. The platform consists of two main backbones: Brillo, an Android-based OS for the development of embedded low-power devices, and Weave, an IoT-oriented communication protocol that serves as the communication language between the device and the cloud.

Calvin is an open source IoT platform released by Ericsson designed for building and managing distributed applications that enable devices to talk to each other. Calvin includes a development framework for application developers, as well as a runtime environment for handling the running application.

DISCUSSION

Consumer and enterprise IoT applications. There are numerous real-world applications of the internet of things, ranging from consumer IoT and enterprise IoT to manufacturing and industrial IoT (IIoT). IoT applications span numerous verticals, including automotive, telecom and energy.

In the consumer segment, for example, smart homes that are equipped with smart thermostats, smart appliances and connected heating, lighting and electronic devices can be controlled remotely via computers and smartphones.

Wearable devices with sensors and software can collect and analyze user data, sending messages to other technologies about the users with the aim of making users' lives easier and more comfortable. Wearable devices are also used for public safety -- for example, improving first responders' response times during emergencies by providing optimized routes to a location or by tracking construction workers' or firefighters' vital signs at life-threatening sites [4].

In healthcare, IoT offers many benefits, including the ability to monitor patients more closely using an analysis of the data that's generated. Hospitals often use IoT systems to complete tasks such as inventory management for both pharmaceuticals and medical instruments.

Smart buildings can, for instance, reduce energy costs using sensors that detect how many occupants are in a room. The temperature can adjust automatically -- for example, turning the air conditioner on if sensors detect a conference room is full or turning the heat down if everyone in the office has gone home.

In agriculture, IoT-based smart farming systems can help monitor, for instance, light, temperature, humidity and soil moisture of crop fields using connected sensors. IoT is also instrumental in automating irrigation systems.

In a smart city, IoT sensors and deployments, such as smart streetlights and smart meters, can help alleviate traffic, conserve energy, monitor and address environmental concerns, and improve sanitation.

IoT security and privacy issues. The internet of things connects billions of devices to the internet and involves the use of billions of data points, all of which need to be secured. Due to its expanded attack surface, IoT security and IoT privacy are cited as major concerns [5].

In 2016, one of the most notorious recent IoT attacks was Mirai, a botnet that infiltrated domain name server provider Dyn and took down many websites for an extended period of time in one of the biggest distributed denial-of-service (DDoS) attacks ever seen. Attackers gained access to the network by exploiting poorly secured IoT devices.

Because IoT devices are closely connected, all a hacker has to do is exploit one vulnerability to manipulate all the data, rendering it unusable. Manufacturers that don't update their devices regularly -- or at all -- leave them vulnerable to cybercriminals.

Additionally, connected devices often ask users to input their personal information, including names, ages, addresses, phone numbers and even social media accounts -- information that's invaluable to hackers.

Hackers aren't the only threat to the internet of things; privacy is another major concern for IoT users. For instance, companies that make and distribute consumer IoT devices could use those devices to obtain and sell users' personal data.

Beyond leaking personal data, IoT poses a risk to critical infrastructure, including electricity, transportation and inancial services.

Smart city construction projects being implemented around the world are being applied as a solution to the problem of socio-economic problems. The technological solutions used should improve, include or include general generic services, reduce the consumption of resources and resources. In article "IoT technologies in smart cities of Uzbekistan" is shown European markets and prospects for smart cities in Uzbekistan.

IT infrastructure has become crucial for a competitive business, a socially stable society and an efficient state. Our world is already global and digitally hyper-connected. This is the world of big data, process automation, digital logistics and personalization, both on the supply and demand sides. Digitalization is the main direction in the development of many states - Germany, China, Japan, the USA, etc. For example, Germany - the ancestor of the Industry 4.0 concept - will soon spend € 5 billion only on developments in the field of artificial intelligence, China plans to invest about $ 1 .4 trillion in information technology by the end of 2025. But the prevailing direction of digital development is the synergy of the digital and physical worlds through the technologies of the Internet of Things or IoT. Countries with developed economies are stimulating this direction through regional strategies for the development of wireless devices [6]. A large number of transnational corporations attract significant financial resources by investing in the latest developments in this area. The Internet of Things is also attractive to small and medium-sized businesses. The technologies of the "Internet of Things" have made it possible to create dynamic networks consisting of billions and trillions of things that communicate and interconnect with each other.

The Internet of Things (IoT) is the process of using digital intelligence in devices that can transmit data in real time without human intervention. These are the billions of physical devices in the lives of people around the world that are connected to the Internet, collect and share data. With cheap processors and wireless networks, you can buy anything from tablets to self-driving cars by connecting to IoT platforms.

The Internet of Things is a new technology that promises to revolutionize areas such as transportation, marketing, hospitality, and more. The basic rule of the "Internet

of Things" is that they are autonomous and interact with each other. The Internet is the common information space and the way things "communicate" with each other.

The concept of "Smart City" arose as a result of the expansion of the potential of the "Internet of things" (IoT). It is modern cities that are becoming experimental sites for the coming digital age. It is important to note that effective development comes down not only to the penetration of "connected" devices into all aspects of human life, but also to the creation of a technological ecosystem that combines technologies for collecting, transmitting, aggregating data on a platform that allows you to process data and use them to implement effective solutions. The combination of the latest IT technologies with urban infrastructure and services promises not only to streamline and improve the lives of citizens, but also save money. Transportation, utilities and security are the main areas where the opportunities of wireless digital technologies are already being successfully applied. Invisible threads of wireless communication entangle the city today, connecting its inhabitants with a huge number of various IoT devices. Smart cities are the most striking example of such technological ecosystem solutions. The idea of a smart city is that the collection and processing of information in a digital mode makes it possible to use available resources with greater productivity and provide residents with better services using IoT technologies. The construction projects of "smart" cities, implemented around the world, are used as an effective method for solving socio-economic problems. Given that more than half of the world's population lives in cities (66%), the issue of implementing and developing the "smart city" system is becoming increasingly important every day. The need for "smart" cities is also associated with the need to increase the level of scientific and technological development of the productive forces, the cultural and socio-spiritual life of society [7]. Due to the importance of the development of smart cities, many countries pay special attention to the formation of policies in the field of technologies of the Internet of things. In the United States in 2016, it was decided to develop a national strategy for the "Internet of Things". South Korea approved in 2014 the "Master Plan for the Internet of Things". Japan adopted the "Japan Growth Strategy" in 2016, which provides for the development of Industry 4.0, "Internet of Things", Big Data. China has already implemented the state program for the development of the Internet of Things until 2020, which was adopted in 2017. The concept of sustainable development involves the introduction of the "Internet of things", Big Data, technologies of "smart" cities in the global economy.

CONCLUSION

IoT ecosystem is pre-mature in terms of security and privacy as these are not prioritized characteristics. Today IoT is being used in almost all sectors like domestic,

industrial, pharma, etc., but the mature state of security is not achieved. Security is not built up from design but rather driven as features. This paper proposes IoT standarts and frameworks based on a systematic review of various published approaches to securing the IoT ecosystem.

REFERENCES:

1. Moore, S. J., Nugent, C. D., Zhang, S., et al. (2020). IoT reliability: A review leading to 5 key research directions. CCF Trans. Pervasive Comp.
2. Khanna, A., & Kaur, S. (2020). Internet of things (IoT), applications and challenges: A comprehensive review. Wireless Personal Communication, 114, 1687–1762.
3. Banda, G., Bommakanti, C. K., & Mohan, H. (2016). One IoT: An IoT protocol and framework for OEMs to make IoT-enabled devices forward compatible. J Reliable Intell Environ, 2, 131–144.
4. Javed, F., Afzal, M. K., Sharif, M., & Kim, B. (2018). Internet of things (IoT) operating systems support, networking technologies, applications, and challenges: A comparative review. IEEE Communications Surveys & Tutorials, 20(3), 2062–2100.
5. Noura, M., Atiquzzaman, M., & Gaedke, M. (2019). Interoperability in internet of things: Taxonomies and open challenges. Mobile Networks and Applications, 24, 796–809.
6. Farooq, M. S., Riaz, S., Abid, A., Umer, T., & Zikria, Y. B. (2020). Role of IoT Technology in Agriculture. A Systematic Literature Review. Electronics, 9(2).
7. Shah, S. H., & Yaqoob, I. (2016). A survey: Internet of things (IOT) technologies, applications and challenges. In 2016 IEEE smart energy grid engineering (SEGE), Oshawa, ON (pp. 381–385).