I.J. Education and Management Engineering, **2018, 6, 24-36**
Published Online November 2018 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2018.06.03

Available online at http://www.mecs-press.net/ijeme

Application and Security Issues of Internet of Things in Oil-Gas Industry

Rashid G. Alakbarov [a], Mammad A. Hashimov [a]

[a] *Institute of Information Technology of ANAS /Department, Baku, AZ1141, Azerbaijan*

Received: 01 June 2018; Accepted: 16 October 2018; Published: 08 November 2018

Abstract

Article proposes an architecture based on new Internet of Things (IoT) for easy, safe, reliable and rapid data collection from sensors installed in oil and gas industry. Use of several Wireless Sensor Networks in management of oil and gas platforms is researched. New opportunities created by processing of data collected via sensors for improvement of safety of oil platforms (deposits), optimization of operations, prevention of problems, troubleshooting and reduction of exploitation costs in oil and gas industry. At the same time, the article analyses safety issues of different layers of monitoring system with IoT architecture.

Index Terms: Internet of Things, Wireless Sensor Networks, monitoring, safety, sensors, smart objects, network gateways, control center.

1. Introduction

In the modern era, the oil and gas complex faces new production problems, especially against the background of a decline in oil prices. Finding new modernized ways to improve results and reduce costs in order to increase efficiency and competitiveness is an urgent and important task. Here a special role is assigned to collection of more detailed and accurate information about the production process and solution of the control problem. Rapid data processing is one of the important directions affecting development of oil and gas industry. Directions such as increasing the speed of exploration and detection of oil, increasing oil production and reducing the risks to health, security of humans and the environment identified as a result of equipment malfunctions or operator errors are constantly developed with application of Internet of Things.

Internet of Things is characterized as the next revolutionary development layer of information technologies

* Corresponding author
E-mail address: rashid@iit.ab.az, mamedhashimov@gmail.com

fields after computer, Internet and mobile telephone communication. IoT is already encountered in each activity field of our daily lives. It is mainly used in medicine, agriculture, Oil-Gas industry and other fields in order to remotely control occurring changes, prevent fires and provision of other useful functionality.

Kevin Ashton, one of the developers of Radio Frequency Identification (RFID) technology notes that, Internet of Things has a potential to change the world as much as Internet, may be even more [1].

Solution of several important social problems is expected with realization of Internet of Things. Also, improvement issues of control development processes in oil and gas industry will be solved.

Internet of Things will affect everything that surrounds us in nearest decades. Mentioned technology is mainly applied in following fields [2]:

- Oil-Gas industry: control of oil products exploration, production, processing, transportation and sale processes;
- In cities: transport control, lighting, stops, smart office buildings, waste control;
- In cars: predictive maintenance support, collision control, self-controlling devices;
- Energy production and distribution: smart grid, microgrid, electrical stations control systems;
- Agriculture: efficient production, situation based irrigation and fertilization;
- Environment: pre-detection of forest fires, tracking animals that are becoming extinct;
- Medicine: remote diagnostics, monitoring of old and sick individuals;

Oil-Gas industry covers expedition, production, processing, transportation and sale processes of oil products. Fuel, oil and gasoline form the majority of products of this industry. Oil is also the raw material for many chemical products, including drug preparations, solutions, fertilizers, pesticides and plastic production. As demand for natural fuel is increasing daily, oil and gas companies must create new technologies and improve operations for increased productivity.

Application of IoT, which is based on sensors, can be taken as a topical issue as the way of implementing the right strategy in gathering information in the oil and gas sector. Application of this technology will enable to control efficiency, make efficient decisions, improve production and increase competitiveness. Oil-Gas industry is the main industry controlling many other industries, important for worldwide energy production and significantly affecting world economy as a result [3].

According to the forecasts of the International Data Corporation (IDC) in the world, global expenses for IoT with an annual growth rate of 15.6% compared to 2015-2020 in 2020 will reach 1.29 trillion dollars. In an analytical study conducted by Gartner it was stated that 307 million sensor units were installed in the productions in only April 2015. These statistical data confirms the urgency of this problem once more. According to calculations of International Data Corporation, number of used IoT devices is expected to reach 41 billion in 2020[4].

Main results of IoT technologies for oil and gas industry are following:

- IoT has several significantly important potential applications in facility exploration, excavation and production operations, maintenance and overall facility control.
- Works on application of IoT technologies in oil and gas field are on experimental level for now and performed works are focused on intensive processing of data and effective control of entrance/exit loadings.

Main objectives of IoT technologies' application are as following:

- Detection of more hydrocarbon deposits;
- Safe, efficient production and transportation with minimal ecological impact ;
- More efficient and cost saving processing and product distribution;
- Planning of optimization;

- Customer relations management;
- Identification of new opportunities and markets.

The second part of the article analyzes the research works on the application of IoT technologies in the oil and gas industry and safety issues. Section 3 reviews the solution of some scientific-theoretical and technological problems with the application of IoT technologies in the oil and gas complex. Section 4 deals with the development of IoT-based architecture for the monitoring of the oil and gas industry's production process. In Section 5, the use of wireless sensors used for monitoring of the oil and gas industry has been substantiated. Section 6 reviews the security issues at different layers of the network.

2. Related Works

Article [5] analyzed the advantages of applying Internet of Things for the efficient monitoring of oil and gas systems. Article [6] offers an oil wells control system based on the architecture of the Internet of Things (sensor, network and application layers). Article [7] reviews the application of Internet of Things technologies in the oil equipment production industry. Article [8] examines analysis of the large-scale data received from the sensors installed on pipelines using Big Data technologies. Article [9] has identified technical requirements for the use of wireless technologies in the oil and gas industry. Due to rapid development of wireless technology, it is more appropriate to install the wireless sensors on old platforms performing their last exploitation period in order to optimize production.

Studies conducted in [10, 11] show that changes required in the operation processes of oil and gas production facilities can be the biggest barrier to the introduction of wireless technologies in the oil and gas industry. It should be noted that these problems often arise when the human factor in the adoption of new technologies is ignored. Recently, WSN based different solutions were developed for monitoring of the situation in the oil and gas industry [12], processing facilities [13, 14], pipeline monitoring

[15, 16], corrosion [17], main well monitoring [18], pumping installations [19] 20]. However, as mentioned in the introduction all of them have significant deficiencies and are exposed to many attacks [21, 22]. In article [23], pipelines are monitored by placing the sensors along the pipelines.

3. Application of Internet of Things Technologies In Oil-Gas Complex

As in all sectors of the industry, application of Internet of Things in the oil and gas industry promises great economic hopes. The application of this technology ensures the solution of a number of scientific-theoretical and technological problems [2]:

- Controlling used equipment (engine, pumps, drilling rigs, etc.);
- Optimization of drilling axis replacement;
- Automatic production platform control;
- Early detection of leaks;
- Pipeline monitoring (for the safety of mechanical- physical condition);
- Greater interaction between automation and security devices;
- Tracking staff through geolocation and monitoring of certain security factors (for example, based on immobility for a certain period of time to notify if the staff member has been injured or fallen by determining the user's pulse through smart helmets or anklets);
- Reducing the need for man-made inspections, detecting leaks in real time, as well as measuring various parameters at the entrance of the oil well to optimize parameters through analytics and machine learning.

The technological process of the oil and gas industry can be conditionally divided into three major sectors [24]. The first sector covers exploration drilling and production processes. Here, primarily, potential

underground or underwater crude oil, natural gas deposits and potential hydrocarbon reserves are researched and explored; exploration wells are drilled in the second stage and then hydrocarbon reserves are extracted from hydrocarbon reserves in oil or gas fields. These hydrocarbons allow the extraction of crude oil or crude natural gas to the surface. In the second sector, crude oil or oil products are transported.

Pipelines, rails, trucks, tanks and many other transportation systems are used to extract crude oil and extract hydrocarbons from production and wells to the processing areas where hydrocarbon and oil refining is performed. Later, various products are processed into the third sector. This sector covers crude oil processing and crude natural gas processing and purification. At this stage, petrol or fuel oil, kerosene, aircraft fuel, diesel fuel, heating supplies, oil, lubricants, wax, asphalt, natural gas and liquefied petroleum gas, as well as hundreds of petrochemical products are offered to consumers.

The article considers the application of IoT technologies to monitor the various operations of these sectors of oil and gas industry.

4. Development of the Architecture based on Internet of Things for Monitoring of Oil-Gas Industry

This section presents the IoT (Internet of Things) based architecture for monitoring various operations of the upper, middle and sub-sectors of the oil and gas industry (Figure 1).

The proposed architecture consists of three modules - sensors (smart object modules), network module (gateways) and application (control center) modules [3, 24, 25]. Each module carries out monitoring of various oil field environments related to each other. Three sections of the IOT architecture offered in other sections of the article are explained in detail in their function and interaction. Additionally, possible technologies are proposed that can be applied to ensure the reliability and efficiency of monitoring and other operations in the oil field.

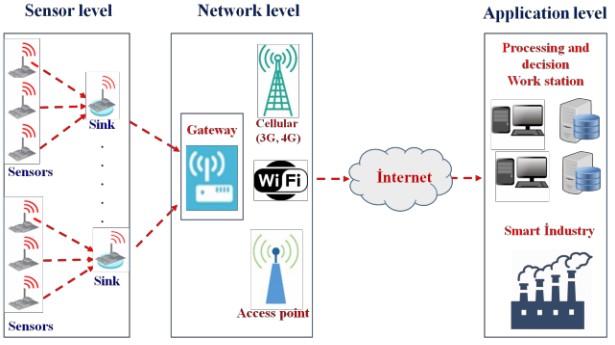

Fig.1. Architecture of Internet of Things Technology

Sensor layer (smart object). Sensor layers consist of sensors installed on different equipment of oil wells and wireless network technologies (3G, 4G, Wi-Fi, ZigBee, etc.) that connect them. Each smart object (sensors) is a physical device, and most of them are placed in different oil equipment. Smart objects allow you to measure and collect data. Installation of a group of Smart objects on different equipment in oilfield environment is called Smart Oilfield. Signals received from sensors installed for monitoring of oil field pumps (pressure and temperature of pumps, pump outlet, etc.) mainly assists the control process [6].

Information collected from oil fields should be transmitted to the server for processing and analysis. Smart object module consists of three layers - sensor, network and application layers. Sensor-layer data is collected and a connection between the smart object and network transitions (gateways) is established. Each smart object is equipped with different types of sensors such as acoustics, temperature, pressure, etc., in order to detect any leaks on it. [25]. The network layer is responsible for establishing communication between the smart object, the

gateway and the control center. Each smart object, as well as other smart objects and networks, provides a quick connection [24].

Network layer (gateways). The network layer is also known as a transmitter layer and is used as an intermediate layer in the Internet architecture of items [26]. The gateway layer basically assures that the data collected on the oil platform is conveyed to the IoT control center or vice versa provides safe transmission of received signals from control center to the sensor layer. Created network controls the installed oil wells devices in several areas, based on the WLAN (Wireless Local Area Network) protocol. In this layer, data is received from the sensor node and if necessary, is encrypted and transmitted to the control center. Because the wells in the oil industry are located far from the center, there is usually no 4G network in these areas and therefore it is important to set up a dedicated wireless network to support the system's service [6].

The network layer (access point) acts as a bridge between the smart object and control center. This module can perform application layer functions when the smart object module does not have the application layer. smart object sets can be connected to the network access point through wireless communications. The network access point is voluntary, but each network connection can be equipped with different sensor types, such as acoustic, temperature and pressure sensors. Communication between the smart object and network access point can be established using standard protocol. Applications running in smart objects and access points including oil and gas leakage, fire etc., allow to take real-time actions against anomalous events (fire alarm, switching off various equipment, evacuation of workers and localization of malfunctions) [24].

Application layer (control center). The application layer is implemented as the top layer of the Internet of Things. The Control Center (server) module responds to application control and analysis of data collected from smart object modules. At this layer, automated control of oil pump monitoring is carried out on the basis of the data control and analysis on each well. It collects data and makes important decisions for anomaly events and supports the decision-making process of the control panel. The control center consists of only two layers - network and application layers. The network layer is responsible for the communication between the smart object and control center through communication technologies. The application layer is largely responsible for managing processes and consists of object interfaces, central IoT control servers, IoT applications, databases, visualization tools etc.

The IoT control center receives data from sensors installed on pumps in real time. The collected data (oil well temperature, pressure, flow, etc.) is analyzed through a smart application and management is performed without human intervention after grouping according to types [6]. The Control Center has two primary goals: to analyze information transmitted to the control center from smart objects through different sensors on the state of equipment, detect malfunctions or predict the possibility of their occurrence. Thus, the control center will assist in the implementation of preventive measures to increase productivity and minimize malfunctions, thereby facilitating better control and maintenance of equipment with lower health and safety risks. The second is to analyze data on production performance based on the daily use and production of oil and gas in the control center [24].

Use of Big Data technologies on IoT. One of the most distinct aspects of IoT is the fact that the data is received from different sources and when the number of these sources (sensors) is quite large the amount of obtained information is excessive.

On the other hand, information from external devices which typically includes business information, asset usage information, geographic information, weather information etc. must be merged with external sources of data to provide useful services. As a result, data quality and control problems also occur. In this case, the integration and processing of heterogeneous IoT data obtained from different sources is of crucial importance. Thus, if these data are not integrated and passed through the initial cleaning process, the next layers - data transmission, storage, and analysis are a great challenge. Thus, as is well-known from the literature, the initial processing of the data (in particular, large-scale) is of crucial importance in its analysis. In this case, there is a

need for new methods for the initial processing of data.

The application of the sensors in the oil and gas industry allows measuring temperature, pressure, and other parameters in the well every 100 m, 10 m, 1 m, and even 10 cm. It is possible to control the well operation and its condition in real-time through the use of sensors in the pipeline. The daily volume of data received from such sensors in just one well reaches several terabytes [8]. It is important to predict possible stops in drilling by using Big Data Analysis technologies. For example, it should be noted that drilling anomalies as a result of large data analysis can save millions of labor and equipment costs only. In other words, the analysis of the data acquired from IoT and the acquisition of new knowledge by using large data analysis technologies can dramatically reduce costs in the oil and gas industry [27]. It is known that large data analysis is complicated and requires considerable memory and computing resources. It is almost impossible to solve this problem with the help of classic methods and available computer technology. We need methods and algorithms that can perform big data analysis with the help of existing computer and network technologies.

5. Application of Wireless Sensor Networks In Oil-Gas Industry

The development of the Internet of Things technology is related to wireless sensor networks (WSN). WSN used in the first layer of the network was examined in this section. Anomaly detection systems used for monitoring of the oil and gas industry include SCADA (Supervisory Control and Data Acquisition) systems. SCADA systems are very expensive, non-flexible, non-scalable, and provide long delays in information provision. Effective measurement and monitoring of certain parameters (temperature, pressure, flow, etc.) are essential for the safety and optimization of processes in the oil and gas industry. Although wired sensors are widely used for this purpose, its operation and maintenance are very difficult and require considerable costs [28]. WSN technology is a new alternative that significantly reduces costs, facilitates exploitation, flexibility and convenience.

During the above processes, there is a need for a wide range of monitoring of various parameters with the help of a large number of sensors. These sensors are installed in different locations for measuring various information about the operation process and operating environment. This is very important for the safety of the production process, production, maintenance plan, optimization of erosion and recovery processes. Sensors, which have been used for many years, have been effectively utilized by cable cables. Operation, management and maintenance of these sensing sensors are very costly, do not fit into temporary installations, and it is difficult to set up in conflicting and remote environments [9, 29]. WSN technology offers faster, less costly, more flexible, and more convenient choices for monitoring systems. Improvements in the Internet, communication and information technology have also contributed to the development of WSN [30, 31].

The hardware component of the sensors consists of a monitoring element (transmitter), an analog-code converter, a memory and a processor, a radio interface element. The monitoring element (transmitter) receives and collects non-electrical parameters of the environment and transmits it to the transmitter. The dialer digitizes and encodes incoming signals. The processing junction consists of memory and processor junction. The processor performs the initial processing of information on certain algorithms and transmits the radio to the network gateway via the interface. The gateway transforms the sensor data into a common-use network protocol and transmits it to the management center's server.

WSN can be used in data collection, monitoring and surveillance systems. Typically, the sensors is used for measuring temperature, pressure, humidity, soil composition, noise levels, lighting conditions, presence of harmful substances in some object etc. [32]. The monitoring in oil and gas industry widely uses temperature, pressure, vibration, motion and flow sensors [29].

Because the sensors are easier, smaller, lighter, and cheaper, WSN is widely applied in automation of oil and gas industry. The most commonly followed parameters include heat, pressure, level, and flow. Other parameters include accommodation, proximity, descriptions and security. In general, these parameters are very useful for automating production and process control [33]. The future application of WSN is considered to be very promising.

Sensor network's main components are as following [13]:

- Set of distributed sensors
- Wireless network connecting sensors to each other
- Calculation node performing initial processing and control of data.

The nodes in the sensor network usually have one or more sensors, radio transmitters, or other wireless communications devices, small microcontrollers and an energy source, usually a battery [34]. Therefore, the new IoT-based architecture is widely used in recent years for easy, secure, powerful, reliable and fast data collection from sensors (objects) installed in the oil and gas industry. Efficient management of production processes with WSN applications is one of the topical issues. These applications can be used for remote monitoring of pipelines, natural gas leakage, corrosion, equipment status and warehouse in real time. Information collected through such sensors opens up new opportunities for innovative solutions and business ventures to help improve the oil and gas platform security, optimize operations, prevent problems, reduce errors and reduces operating costs. This article explores the use of a number of WSN applications in the oil and gas industry.

Advantages of WSN technology for monitoring in the oil and gas industry include:

- The latest achievements in wireless technology have led to the creation of cheap wireless networks that, basically, provide strong and reliable communication. Sets are used in the key features of international standards of wireless sensor networks such as ZigBee PRO [35], Wireless HART [36] and ISA100.11a [37] to provide a layered and concise description of the network protocol structure.
- Wireless technology has many possibilities [9]. Eliminating the need for power supply can help reduce installation and maintenance costs. It allows installing devices in remote areas and application of expensive, temporary and mobile systems.
- Networks can consist of sensors that detect various types of signs (pressure, temperature, fire, humidity, vibration, soil composition, etc.) that monitor the different environments listed below, such as seismic, thermal, visual, acoustic, radar, magnetic, infrared, etc. [38].
- Recently, wireless sensors have been applied in a wide range of fields with different demands and features (glacier monitoring, ocean water monitoring, landslide rescue service, monitoring of energy systems, monitoring of objects etc.) [34].

There are some difficulties with the application of wireless devices in the oil and gas industry. Wireless devices must have the following features [6];

- Small size, limited processing power, memory, storage other capabilities.
- Self-reliance. Whenever possible, installations must supply their own power and have several long-term battery packages to reduce the demand for technical support.
- Have an opportunity to work in disputed areas where environmental and platform conditions are very severe.
- It should be seamlessly integrated with existing IT solutions.
- Be self-configurable, dynamic and adaptive.
- Be able to serve in a dynamically changing system environment.
- Must be error-proof and restorable.
- Must be based on transparent, international standards.
- Precisely designated operational reliability and availability of an existing wireless network within an operational environment.

Problems with sensors used in Wireless Sensor Networks Technologies:

- Sensors have limited energy
- Sensors produced by different manufacturers interact with the Internet of Things, but currently there are no international standards for marking the sensors.
- Physical sensitivity of the sensors and so on.

6. Safety Issues

The services provided by IoT applications can greatly risk personal privacy and security, as well as have great benefits to human life. Experts in the security sector have repeatedly warned of the potential risks of a multiple dangerous devices with an Internet connection, as IoT manufacturers could not apply a stable security system on their devices. Each layer of the IoT architecture is sensitive to security threats and attacks. These attacks can be either active or passive, resulting from an attack from external sources and internal networks. Active attack stops direct service, and passive attack controls network information without stopping service. At each layer, IoT's device and services are sensitive to DoS attacks. These types of attacks prevent authorized users from using device, resource or network [39]. The following sections provide a detailed analysis of security issues for each layer.

6.1. Sensor Level Security Issues

There are three security issues at the sensor layer [39]. The first issue is related to power of wireless signals. Alarms are mainly transmitted through the use of wireless technology between sensor nodes. In this case, effectiveness can be exposed by external waves. The second issue is that it can be interfered with by the attackers not only by the owner, but also by the attackers at the sensor junction on IoT devices. Thus, the operation of the intersections in the external and outdoor environments causes sensors and devices to be exposed to physical attacks. This can result in attackers interfering with hardware components. The third issue is related to the characteristic dynamics of the network topology. Thus, the location of the IoT nodes is often changed. IoT sensor level is mainly composed of sensors and RFIDs. Their storage capacity, energy consumption, and computing capabilities are very limited and can be sensitive to many threats and attacks.

Node Capture Attacks –Many installations are statically placed in the sites, which can cause them to be physically endangered [40]. If any node is attacked, important data (group communication key, radio switch, compatibility signal, etc.) can be captured by an attacker. The attacker may also transfer all important information about the seized node to the damaged node and may then display the damaged node as a permitted node in order to connect to a network or a system. This attack is also expressed as an node replication attack. An node attack can have a serious impact on the network. Effective schemes should be studied in the field of monitoring and detection of malicious nodes to prevent such attacks.

Malicious code Injection Attacks –In addition to the capture attack of the node, the attacker can control the device by entering a malicious code in its memory. This malicious code does not only perform specific functions, but also provides the attacker's access to IoT System and even ensure his full control over IoT system [41]. In order to protect against malicious code attack, it is necessary to design effective code identification schemes and integrate them into IoT.

False Data Injection Attacks – By capturing the node or devices in IoT, attacker may place false information and transmit false information to IoT applications instead of normal information received from the node or the device. After receiving false information, IoT programs can send incorrect feedback commands or provide

incorrect services, which can affect the efficiency of IoT software and networks. In order to be protected from such a malicious attack, efficient methods must be developed that can identify and return false information before its reception by IoT applications (fraudulent data filtering scheme, etc.) [42].

Sleep Deprivation Attacks - Most of the devices or nodes in the IoT have fewer electrical capabilities. Device or nodes are designed to extend the life of devices and nodes so that it is possible to apply sleep mode to reduce their energy consumption. However, sleep deprivation attack can impair programmed sleep patterns, which can lead to uninterrupted operation of the device until its shutdown [40]. There is a way to extend the life of these devices and nodes, which is their ability to accumulate energy from the outside (sun, wind, etc.).

6.2. Network Level Security Issues

Since the main purpose of the network layer in IoT is to transmit the collected data, security issues at this layer are based on the impact of network resources. In addition, most IoT devices connect to IoT networks through wireless communication. Thus, most security issues at this layer are related to wireless networks.

Denial-of-service Attacks - DoS attacks can disable IoT system services by attacking network protocols or by loading network with excessive traffic. DoS attack is one of the most common attacks. So DoS attacks, Ping of Death, TearDrop, UDP, SYN, Land Attack and others can be using attack schemes [42]. In order to protect against the DoS attacks, the attack schemes must first be carefully examined and then effective defense schemes should be created to minimize attacks in order to ensure the security of the IoT systems.

Spoofing Attacks –The purpose of spoofing attacks is to ensure that the attacker has full access to the IoT system and to send malicious information to the system. IP spoofing, RFID spoofing etc. are example of IoT spoofing attacks. IP spoofing attack can falsify and record a valid IP address in other permitted devices on the attacking network. Later on, it can access the IoT system and send malicious information through trusted IP addresses showing them as valid information. During RFID spoofing attack the attacker can secretly store and record information about a valid RFID badge and then send malicious information to the IoT system with that valid ID badge (identification) [40, 42]. Safe reliable control, identification and authentication solutions can be used to protect against spoofing attacks [42].

Sinkhole Attacks - During this attack the attackers provides that the malicious node looks attractive to other nodes. Thus, all information flow coming from a specific node is directed to a malicious node, which causes package drop, i.e. all traffic is stopped and system believes that the other side accepted the information [40]. It must be noted that, sinkhole attack is not only organized to disrupt confidentiality of delivered information, it can also perform additional attacks (DoS attack etc.). This leads to greater energy consumption. Methods such as safe routing protocol can be researched and applied for protection from sinkhole attack.

Man-in-the-middle Attack - In this case, the malicious device controlled by the attacker can be virtually located on the network between two communication devices. The malicious device can save and direct all data transmitted between the two devices by stealing the identification data of two normal devices [43]. These two normal devices are unable to detect the device between them and even believe that they are communicating directly with each other. This attack can disrupt the privacy, integrity and confidentiality of the information contained in IoT by watching, listening, distorting, and monitoring the connection between the two normal devices. In contrast to the physical attacks of devices over hardware, this attack can only be carried out based on communications protocols used in IoT networks. Effective protection methods include safe communication protocols and key management schemes that ensure that normal devices are not detected by the attacker and that the key data is not leaked [42].

Routing Information Attacks – These attacks are mainly focused on routing protocols in IoT systems. Here routing information can be manipulated by an attacker and can be resent thus creating a loop on the network. This can cause swelling of the source information and increased delays in the IoT network. Secure routing protocols and secure management can be used to secure the connection between devices for the purpose of protection against this attack, as well as for not to leak identification information and IP addresses to attackers [42].

Sybil Attacks - During the sybil attack, any malicious device, i.e. sybil device, provides several identifications to other nodes on the network, and thus the attacker can also be located in many places simultaneously [43]. Since the sybil device has a number of legitimate identifiers, false information sent by the sybil device can be easily accessed by neighboring devices. Additionally, the routes that selected the sybil device as a routing node can suppose that several different crossing paths are identified. In fact, only one route is identified and all data transmitted is required to pass through the device. Safer identification and authentication mechanisms should be developed to protect against sybil attacks.

Unauthorized Access– RFID is one of the most important technologies in the IoT. As the majority of RFID-based devices are integrated into the IoT, and most RFIDs lack proper identification mechanisms, the attacker can access RFID tags and information stored there can be retrieved, modified and erased. Thus, the further development of the RFID-based devices' access and authentication mechanisms in IoT much be achieved [42].

6.3. Safety issues of application layer

The main purpose of the application layer is to support any request sent by users. Thus, application-layer problems are related to software attacks. Here are some of the possible problems with the application layer:

Phishing Attack – It can confiscate users' confidential information, such as identities and passwords, by fraudulent identification information through infected e- mail and phishing websites [41]. Secure authorization, authentication and authentication may reduce phishing attacks. [42].

Malicious Virus/worm – One of the other problems for IoT applications is malicious virus or worms. Attacker can detect or distort confidential information by infecting IoT programs with malicious (Trojan, Trojan, etc.) viruses [40]. Reliable firewall, virus detection, and other protection mechanisms should be deployed to combat malicious virus or worm attacks on IoT applications.

Malicious Scripts - Malicious scripts are added to the software to deteriorate the functionality of the IoT system, make changes to the software, and are removed from the software. Since all IoT applications are connected to the Internet, they can easily deceive customers who require services through internet using malicious scripts (java attack programs, active-x scripts, etc.). Malicious scripts may cause hidden data leakage and even a complete system shutdown. In order to be protected from malicious scripts, static code and dynamic behavior detection methods should be used in the IoT system including effective script detection methods and honeypot techniques [42].

7. Conclusion

The article recommends a monitoring system based Internet of Things technology to improve the safety of oil platforms (deposits), optimization of operations, preventing emerging problems, eliminating errors and reducing operational costs based on data collected through sensors in the oil and gas industry. It has been noted that the use of wireless Internet of Things technologies in the sensory network technology has a significant impact on costs' reduction, simplification of exploitation, flexibility and convenience. The issues of ensuring the solution of a number of scientific-theoretical and technological problems in the oil and gas industry through the application of the Internet technologies of items have been analyzed. At the same time, security issues

emerging at different layers of the proposed architecture have also been analyzed.

Acknowledgment

This work was financed by the Scientific Fund of the State Oil Company of the Republic of Azerbaijan – **Grant – N01 LR**

References

[1] R.M. Aliguliyev, R.S. Mahmudov, Internet of Things: essence, opportunities and problems, problems of the Information Society, 2011, №2(4), pp.29-40.
[2] C.R. Baudoin, Deploying the Industrial Internet in Oil & Gas: Challenges and Opportunities. Society of Petroleum Engineers, 2016, pp.1-11.
[3] M.R. Akhondi, A. Talevski, S. Carlsen and S. Petersen. Applications of Wireless Sensor Networks in the Oil, Gas and Resources Industries in 24th IEEE International Conference on Advanced Information Networking and Applications. pp. 618-623, 2010
[4] M.A. Hashimov, Security issues of the Internet of Things, "Topical problems of information security" III Republican scientific-practical seminar, 08 December, pp. 108-111, 2017.
[5] M. Abdelhafidh, M. Fourati, L.C Fourati and A. Chouaya, İnternet of things in industry 4.0 case study: fluid distribution monitoring system, Computer Science & Information Technology, 2017, pp. 1-11.
[6] S. Yang, C. Gong. Research of Petroleum Well Fuel Pump Measurement & Control System Based on Internet of Things Technology, International Conference on Computer Network, Electronic and Automation, 2017, pp. 410-416.
[7] H. Song, H. Xin-zhou, D. Li, "Petroleum equipment manufacturing industry in the internet of things technology application," Manufacturing Automation, 2013, vol. 35, pp. 63-67.
[8] R.M. Aliguliyev, Y.N. Imamverdiyev, Conceptual Big Data architecture for Oil-Gas induistry, problems of the Information Society, 2017, №1, pp. 3–14.
[9] S. Petersen, P. Doyle, S. Vatland, C. S. Aasland, T. M. Andersen, and S. Dag. Emerging Technologies and Factory Automation, ETFA. IEEE Conference on, Requirements, drivers and analysis of wireless sensor network solutions for the Oil & Gas industry, 2007. pp 102-114.
[10] S. Carlsen, S. Petersen, A. Skavhaug, and P. Doyle, "Using Wireless Sensor Networks to Enable Increased Oil Recovery", Proceedings of the 13th IEEE International Conference on Emerging Technologies and Factory Automation, Hamburg, Germany, Sept. 15-18, pp. 1039- 1048, 2008.
[11] S. Petersen, et al., "A Survey of Wireless Technology for the Oil & Gas Industry", Proceedings of the SPE Smart Energy Conference, 25-27 Feb. 2008.
[12] G. Minetti. "Wireless Sensor Networks Enable Remote Condition Monitoring." Pipeline & Gas Journal 239, no. 7 (2012): 53-54.
[13] A.O. Adejo, A.J Onumanyi, J.M Anyanya and S.O Oyewobi, Oil And Gas Process Monitoring Throughwireless Sensor Networks: A Survey. Ozean Journal of Applied Science, 2013, 6(2).
[14] S.Savazzi, S.Guardiano and U.Spagnolini. Wireless sensor network modeling and deployment challenges in oil and gas refinery plants. International Journal of Distributed Sensor Networks, 2013.
[15] Cegla, Frederic, and Jon Allin. "Ultrasonic Monitoring of Pipeline Wall Thickness with Autonomous, Wireless Sensor Networks." Oil and Gas Pipelines: Integrity and Safety Handbook: 2015, pp. 571-578.
[16] G.C. Nwalozie, A.C.O Azubogu, A.C Okafor, Alagbu, "Pipeline Monitoring System Using Acceleration-Based Wireless Sensor Network",E E. IUP Journal of Telecommunications7.2: May 2015, pp. 42-58.
[17] Hozoi, Adrian, Zoltan Papp, and Peter van der Mark. "Sensor Network for Corrosion Monitoring."

Wireless Sensor Network: 28.

[18] Yi, Pan, Lizhi Xiao, and Yuanzhong Zhang. "Remote real- time monitoring system for oil and gas well based on wireless sensor networks." In Mechanic Automation and Control Engineering (MACE), 2010 International Conference on, pp. 2427-2429. IEEE, 2010.

[19] Gao, Meijuan, J. Xu and J. Tian. "Remote monitoring system of pumping unit based on wireless sensor networks." In Industrial Technology, 2008. ICIT 2008. IEEE International Conference on, pp. 1- 4. IEEE, 2008.

[20] Xu, Qinghua, Jinyu Jiang, and Xianbiao Wang. "Research and Development of Oil Drilling Monitoring System Based on Wireless Sensor Network Technology." In Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC'09. International Conference on, vol. 2, pp. 326-329. IEEE, 2009.

[21] Khan, W. Z., Aalsalem, M. Y., Saad, N. M., Xaing, Y., & Luan, T. H. (2014, April). Detecting replicated nodes in wireless sensor networks using random walks and network division. In Wireless Communications and Networking Conference (WCNC), IEEE, pp. 2623-2628, 2014.

[22] Y. Zeng, J. Cao, S. Zhang, S. Guo, & L. Xi, Random-walk based approach to detect clone attacks in wireless sensor networks. Selected Areas in Communications, IEEE Journal on, 2010. 28(5), pp. 677-691.

[23] Allison, S. Peter, E. Charles, Chassaing and B. Lethcoe, "Acoustic impact detection and monitoring system." U.S. Patent 7,607,351, issued October 27, 2009.

[24] W.Z. Khan, M.Y. Aalsalem, M.K. Khan, M.S. Hossain, M. Atiquzzaman, A Reliable Internet of Things based Architecture for Oil and Gas Industry. 19th International Conference on Advanced Communication Technology, 2017, pp. 705 – 710.

[25] K.K. Patel, S.M. Patel, Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. International Journal of Engineering Science and Computing. May 2016, Volume 6 Issue No. 5. pp. 6122-6133.

[26] M. Wu, T.l. Lu, F.Y Ling, J. Sun and H.Y. Du, Research on the architecture of Internet of things, 3rd International Conference on Advanced Computer Theory and Engineering, pp. 484-487. 2010.

[27] K.R. Kundhavai, S. Sridevi, IoT and Big Data- The Current and Future Technologies: A Review. International Journal of Computer Science and Mobile Computing. January- 2016, Vol.5 Issue.1, pp. 10-14.

[28] Boyer, A. Stuart, SCADA: supervisory control and data acquisition. International Society of Automation, 2009.

[29] A. Talevski, S. Carlsen and S. Petersen, Research Challenges in Applying Smart Wireless Sensors in the Oil, Gas and Resources Industries, 7th IEEE International Conference on Industrial Informatics (INDIN 2009), 2009.

[30] K. Sohraby, D. Minoli and T. Znati, Wireless sensor networks: technology, protocols, and applications. Published by John Wiley & Sons, Inc., Hoboken, New Jersey, ISBN: 978-0-471-74300-2. 2007.

[31] Yick, B. Mukherjee and D. Ghosal, Wireless sensor network survey in Elsevier Journal of Computer Networks.www.elsevier.com/locate/comnet. 2008.

[32] A.S.K. Pathan, H.W. Lee and C.S. Hong, Security in wireless sensor networks: issues and challenges, The 8th International Conference on Advanced Communication Technology, ICACT. Conference Publications Page(s): pp. 1043–1048. Feb. 20-22, 2006.

[33] Marketresearch, Industrial Wireless Sensor Networks (IWSN) Market – Global Forecast & Analysis (2012– 2017) June 19, Accessed 20-12-2012 from http://www.marketresearch.com/MarketsandMarketsv3719/Industrial-Wireless-Sensor Networks-IWSN-7030069/, 2012.

[34] K. Römer, and F. Mattern, "The Design Space of Wireless Sensor Networks", IEEE Wireless Communications 11 (6): 54–61, doi:10.1109/MWC.2004.1368897. December 2004.

[35] ZigBee Alliance, "ZigBee PRO Specification", Standard, Oct. 2007.

[36] HART Communication Foundation, “HART Field Communication Protocol Specification, Revision 7.0”, Standard, Sept. 2007.
[37] ISA100 Standards Committee, “ISA100.11a-2009 Wireless systems for industrial automation: Process control and related applications”, Standard, Sept. 2009.
[38] I.F. Akyildiz, W. Su Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey. *Computer Networks* 2002, 38 (4): pp. 393- 422.
[39] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures, The 10th International Conference for Internet Technology and Secured Transactions, pp. 336-341, 2015.
[40] B.Sasikala, M. Rajanarajana, B. Geethavani, Internet of Things: A Survey on Security Issues Analysis and Countermeasures, International Journal Of Engineering And Computer Science, 2017, vol.6, no.5, pp. 21435- 21442,
[41] M.U. Farooq, M. Waseem, A. Khairi, S. Mazhar, A Critical Analysis on the Security Concerns of Internet of Things (IoT), International Journal of Computer Applications, 2015, vol.111, no.7, pp. 1-6.
[42] J. Lin, W. Yuy, N. Zhangz, X. Yang, H. Zhangx and W. Zhao, A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, IEEE Internet of Things Journal, 2017, vol.4, no.5, pp. 1125–1142.
[43] E. Leloglu, A Review of Security Concerns in Internet of Things, Journal of Computer and Communications, 2017, vol.5, pp. 121-136.

Authors’ Profiles

Rashid G. Alakbarov graduated fromAutomation and Computer Engineering‖ faculty of Azerbaijan Polytechnic University named after C.Ildirim. He received his PhD degree in 2006 from Supreme Attestation Commission under the President of the Republic of Azerbaijan. His primary research interests include various areas in cloud computing, data processing, computer networks, virtual computing, particularly in the area of distributed computing. He is head of department at the Institute of Information Technology as of 2002. Since 2010, he has been leading the development of "AzScienceNet" infrastructure. In 2011, he was appointed a deputy director of the institute by the decision of the Presidium of Azerbaijan National Academy of Sciences. He is the author of 70 scientific papers, including 5 inventions

Mammad A. Hashimov received his Master’s degree in automation and control from Azerbaijan Technical University in Baku, Azerbaijan. He received his PhD degree in 2006 from Supreme Attestation Commission under the President of the Republic of Azerbaijan. He is scientific researcher of Institute of Information Technology of Azerbaijan National Academy of Sciences. His primary research interests include various areas in internet of things, cloud computing, data processing, computer networks, virtual computing, particularly in the area of cloud technology applications. He is the author of 8 journal scientific papers and 16 proceedings.

How to cite this paper: Rashid G. Alakbarov, Mammad A. Hashimov,"Application and Security Issues of Internet of Things in Oil-Gas Industry", International Journal of Education and Management Engineering(IJEME), Vol.8, No.6, pp.24-36, 2018.DOI: 10.5815/ijeme.2018.06.03