COIA 2022

PROCEEDINGS

of the
8th International Conference on

CONTROL AND OPTIMIZATION WITH INDUSTRIAL APPLICATIONS

Volume II

24-26 August, 2022
Baku, Azerbaijan

ISBN 978 – 9952 – 37 – 860 – 3
ISBN 978 – 9952 – 37 – 862 – 7 (Volume II)

MINISTRY OF DIGITAL DEVELOPMENT
AND TRANSPORT
OF THE REPUBLIC OF AZERBAIJAN

BAKI DÖVLƏT UNİVERSİTETİ
BDU
1919
BAKU STATE UNIVERSITY

IAM
Institute of Applied Mathematics

The 8th International Conference on Control and Optimization with Industrial Applications, 24-26 August 2022, Baku, Azerbaijan

FOG COMPUTING APPLICATION IN OIL AND GAS INDUSTRY AND ANALYSIS OF CYBERSECURITY PROBLEMS*

R.G. ALAKBAROV[1], M.A. HASHIMOV[1]

[1]Institute of Information Technology of ANAS, Baku, Azerbaijan
e-mail: muavini@iit.science.az, mamedhashimov@gmail.com

1. Introduction

Operational data management can be estimated as one of the important areas affecting the development of the oil and gas industry. To increase the speed of oil exploration and detection, and to upsurge the oil production and to reduce the health, safety and environmental risks caused by equipment defects or operator errors, etc. the sensor networks are widely used. The data generated by sensors installed to measure various physical parameters are collected. Cloud Computing (CC) with high computing power and memory capacity is considered to be an effective solution for data processing in this field. Large amounts of data stored in cloud are processed and analyzed. Although CC is an effective technology for processing and storing generated data in a networked environment, the real-time transmission of large amounts of data still faces some problems due to the low network bandwidth. Fog Computing (FC) systems have been widely used in recent years for faster data processing. These systems process the data in the computing nodes located near the devices that generate them, which reduces the bandwidth problems (latency) of the network channel.

2. Advantages of using Fog computing in oil and gas industry

In recent years, there has been a transition to corporate governance systems such as CC and FC. In oil and gas industry, the applications such as SCADA are considered to be more promising in terms of migration to Cloud and Fog environment, potential cost reduction, scaling capabilities and maintenance. Some of the features and advantages of FC technology over cloud technology may include [2]:

(1) Cloud architecture is centralized and consists of large data centers located in different parts of the world, thousands of kilometers away from customers. Whereas Fog architecture is distributed and consists of millions of small nodes located as close as possible to the sources generating the data.

(2) Fog level acts as a mediator between the data source and the cloud. If there is no fog level in the system, the cloud communicates directly with the data sources, which complicates the process management.

(3) Data processing in CC is performed on remote cloud servers. In FC, the data processing and storage is performed in real time at computing nodes located on the edge of the network segment close to the data source.

*This work was supported by the Science Foundation of the State Oil Company of the Azerbaijan Republic (Contract No.3 LR-AMEA).

(4) Cloud consists of several large server nodes. Whereas Fog includes millions of tiny nodes and sensors.

In oil and gas industry, fog technology is mainly used in the following areas:

(1) Pipeline optimization in oil and gas industry (real-time monitoring of pressure, flow, compressor, early detection of leaks, corrosion monitoring);

(2) Monitoring of oil wells' condition (control of drilling rigs, control of power supply voltage and current of oil pumps);

(3) Personnel geolocation tracking and monitoring of certain safety factors (determination of blood sugar by smart helmets or wristbands, electrocardiogram (ECG) monitoring, body temperature monitoring, etc.)

3. Cyber-security problems of Fog computing technology

FC is based on the computing power of distributed nodes in order to reduce the overall load of the data center. Since the nodes generating the data are distributed, centralized control over them becomes complicated. Currently, the Fog Platform is a cybercrime hotspot, primarily due to the lack of centralized management and poorly protected peripheral nodes. In addition, when a new fog node is added to the fog network or the previous node is unable to provide service and needs to be removed from the network, other fog nodes potentially have to change their topologies and reconstruct their communication structures to ensure communication between them. The process of reconstructing the topology causes new security problems.

Some of the potential security threats at different levels of FC technology are listed below [1, 5]:

(1) **Spoofing Attack**: This attack disguises the attacker and sends fake information to the network. Devices on the network receive fake data rather than the original one, which allows attackers to gain full access to the system. For example, IP spoofing. In IP spoofing attack, an attacker can falsify and record a valid IP address available on other licensed devices on the network. It can then log on to the system, send the malicious information as trusted, and send it via trusted IP addresses.

(2) **Malicious Node:** One of the main concerns of Fog Computing is the presence of fake Fog Nodes, which can pose a serious threat to data security and privacy. When added to a network, a fake node infects (disrupts) the entire system by spreading malicious information. This attack can disrupt the operations of the Fog network, collect confidential information, violate the data completeness or availability, and so forth.

(3) **Blackhole Attack**: An invalid routing information is generated and all data packets are routed to a "blackhole". This can cause the network to become overloaded and the packet to be dropped. This makes the attacking node look attractive to other nodes. Thus, all the data flow from any particular node is directed to the unsafe node, which causes packets to be dropped, i.e., all traffic stops and the system believes that the information is received by the opposite side.

(4) **Denial of services, DOS**: Attackers exhaust the resources of a fog node by sending multiple requests to the node using simple communication protocols, consequently causing the equipment to stop working. Since most devices connected to the fog network do not authenticate each other, DoS attack becomes easier to perform. As a result, attackers successfully prevent legitimate users and devices from accessing services provided by the fog node or even the cloud.

Here are some suggested countermeasures to protect data from cyber-attacks in FC environment [3, 4]:

(1) **Decoy technique**. This is a security method used to authenticate user data available on a computer network. It replaces the original information with the false one, which is then passed on to the attackers. When an attacker causes a security breach in the system, he finds

a fake data file instead of the original one. This file is known as a cheat file, and the proposed method is called the Decoy Technique.

(2) **Blockchain technology.** The main reason for the success and importance of blockchain technology is that it is decentralized and allows applications to run in a distributed manner. Obviously, blockchain technology has become a hot topic in recent years, though it is still quite new for Fog environment. However, the safety of fog environment can be improved by using blockchain technology over time.

(3) **Intrusion Detection System (IDS).** An IDS must be installed within the fog network that can integrate the individual scattered detection components. In FC, IDS is used to detect and protect against the attacks, including DoS, internal attacks, port scan attacks, food attacks on virtual machines, man-in-the-middle attacks, hypervisors, and etc.

(4) **Encryption techniques**. With the help of effective encryption methods, the privacy problem can be solved, since the attackers will not be able to decrypt complex encryption algorithms. Recently, Homomorphic Encryption (HE) is gaining more and more attention. HE is a cryptographic technique and performs computing on encrypted data and maintain confidentiality when processing sensitive data.

4. Conclusion

Although fog computing has a number of advantages over cloud computing systems, a number of cybersecurity issues arise when using fog computing. Given that security is one of the key factors in the oil and gas industry, there are hesitations in the application of fog computing in the oil and gas industry due to cybersecurity issues. Therefore, the identification of cyber security problems of fog technologies and the development of methods to combat them is one of the most pressing issues today. New, state-of-the-art security mechanisms are required to address the security and privacy issues arising when applying fog computing. In this regard, this article examines the cyber security problems arising when using fog technology and analyzes the existing methods and tools for their solution. Analyses enable to determine future research trends and develop new methods and algorithms for solving the following problems related to cyber security in fog computing:

- Analysis of the characteristics of individual components of fog computing systems and developing algorithms for their effective application in the oil and gas industry.
- Development of methods and algorithms for detecting fake nodes connected to Fog Computing systems without permission.
- Development of methods and algorithms for protecting Fog systems from DoS attacks.
- Development of methods to protect the fog systems network infrastructure from IP spoofing attacks

Keywords: Oil and Gas Industry, Cloud Computing, Fog Computing, Fog Security.

AMS Subject Classification: 68Mxx.

References

[1] Deepak P., Saraju P.M., Sanjivani A.B., Graham M., Rajiv R., Fog Computing security challenges and future directions, *IEEE Consumer Electronics Magazine*, Vol.8, No.3, 2019, pp.92-96.

[2] Hashimov M.A., Issues of the use of fog technologies in the IoT environment, *Problems of Information Technology,* No.2, 2020, pp.80-90.

[3] Mithun M., Rakesh M., Lei S., Leandros M., Mohamed A.F., Nikumani C., Vikas K., Security and privacy in fog computing: challenges, *IEEE Access,* Vol.5, 2017, pp.19293-19304.

[4] Neelam S.K., Mohammad A.C., Security challenges in Fog and IoT, blockchain technology and cell tree solutions: A Review, *Scalable Computing: Practice and Experience,* Vol.21, No.3, 2020, pp.515-541.

[5] Yehia I.A., Ahmad A.A., Ashraf J., Valmira H.O., FOG Computing architecture, benefits, security, and privacy, for the internet of thing applications: An overview, *Journal of Theoretical and Applied Information Technology,* Vol.99, No.2, 2021, pp.436-451.