DOI: 10.21917/ijct.2024.0482

FOG ENABLED PRIVATE BLOCKCHAIN-BASED IDENTITY AUTHENTICATION SCHEME FOR OIL AND GAS FIELD MONITORING

Abdulla J. Y. Aldarwish[1], Kalyani Patel[2], Aqeel A. Yaseen[3], Ali A. Yassin[4] and Zaid Ameen Abduljabbar[5]

[1,3]Department of Computer Science, Gujarat University, India

[2]Department of Computer Application and Information Technology, K.S. School of Business Management and Information Technology, India

[4,5]Department of Computer Sciences, College of Education for Pure Sciences, University of Basrah, Iraq

Abstract

The oil and gas industry remains critical to the global economy, as it contributes to the provision of energy and raw materials. Nonetheless, this sector continued to face clear challenges in operational effectiveness, risk and security. Regular tracking methods are limited to latency issues; they are not secure, and data may face integrity issues. To this end, this paper lays out an efficient fog-enabled private blockchain-based identity authentication approach for oil and gas field monitoring. By integrating IoT devices to blockchain, , decentralized control systems are created that enhance security, transparency, and efficient execution of transactions. In this scheme, by making full use of the decentralized structure of blockchain technology and applying the computational power of fog nodes, a secure and efficient identity authentication framework is designed. Fog nodes are an intermediary between IoT devices and blockchain technology, providing lower latency in communication, and therefore more efficient. The main contributions of this paper include: developing a decentralized authentication system based on private blockchains and fog nodes to overcome the drawbacks of centralized models. Create a network model using a private blockchain that dramatically improves feasibility by incorporating strict admission and authorization procedures. Hence, this leads to simultaneous registrations with minimal network time consensus Authentication that incorporating fuzzy extractor to connect the privacy-centric approach and to improve the security analysis and performance evaluation proving that the proposed solution provides better. According to the previous security analysis, it is clear that the scheme conflicts with different types of threats including DoS, MITM attacks, replay, Sybil, and message substitution attacks. The performance evaluation also shows low computational and communication costs, high compatibility, and real-time operation, which indicates that the proposed scheme is effective and can be implemented as a real-time oil and gas field monitoring system.

Keywords:

Fog Computing, Blockchain, IIoT, Authentication, Oil and Gas Industry

1. INTRODUCTION

The oil and gas industry is a cornerstone of the global economy, providing essential energy and raw materials. However, this sector faces significant challenges in automation and industrial control. Conventional automation systems in use in the oil and gas sector have several drawbacks, including outdated technology, poor integration, and susceptibility to cyber risks. These systems are inefficient and costly to operate. Failures and disruptions can cause serious safety hazards and financial losses.

Furthermore, the industry is exposed to cyber threats and hacking incidents more than ever. These attacks affect the monitoring and control systems hence opening up the system to unauthorized access, data leak and manipulation of operations. Cyber security threats are a major concern and can lead to significant operational loss and even environmental damage [1], [2]. Such breaches emphasize that there is an intensive need for effective measures to be taken to secure the ICSs within the oil and gas industry. Thus, it is important to provide a high level of cybersecurity to minimize the negative impact on the operation and prevent possible disastrous consequences.

Failures and weaknesses in security systems are often due to authentication mechanisms that are not suitable for the Internet of Things (IoT) [3]-[4]. Traditional authentication systems are centralized, making them vulnerable to single points of failure and scalability issues. In an IoT environment, where numerous devices need to communicate securely, centralized systems cannot handle the load efficiently. This results in slow response times and increased vulnerability to attacks. The centralized nature of these systems also makes them an attractive target for cyber attackers, who can compromise the entire network by attacking a single point [5]-[6]. Therefore, there is a critical need for decentralized and scalable authentication mechanisms to ensure robust security in IoT-based industrial environments like the oil and gas industry.

Decentralization in the application of protection for automation and monitoring systems addresses many issues associated with centralized systems. Decentralized systems distribute control across multiple nodes, reducing the risk of a single point of failure. This enhances the resilience of the system and improves its ability to handle large-scale operations typical of the IoT environment. By distributing the workload, decentralized systems can manage higher volumes of data and ensure more reliable and efficient operations [7]-[9].

Blockchain technology is employed to cover some of the drawbacks of centralization problems. Blockchain provides a decentralized ledger that records transactions in a secure and transparent manner. This technology ensures data integrity and prevents unauthorized tampering. In the context of the industry, blockchain can be used to secure communication between IoT devices and ensure that all transactions are verified and immutable. This reduces the risk of data breaches and enhances the overall security of the system.

However, decentralization also suffers from failures and problems. One significant issue is the complexity of managing a decentralized network [9]. Ensuring consistent data synchronization across all nodes can be challenging. Additionally, decentralized systems may face higher latency due to the need for consensus mechanisms to validate transactions [10]. This can impact the speed of operations, especially in time-sensitive environments like oil and gas field monitoring. Another problem is the potential for scalability issues as the number of