SUGISAKA MASANORI

Journal of Robotics, Networking and Artificial Life
Vol. 11(1); May (2025), pp. 69–72
ISSN (Online): 2352-6386; ISSN (Print): 2405-9021
https://alife-robotics.org/jrnal.html

Research Article

DamChain: A Dam Warning System Based on Blockchain

I-Hsien Liu[1], YingCheng Wu[1], Chu-Fen Li[2], Jung-Shian Li[1]
[1]*National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan*
[2]*National Formosa University, No.64, Wunhua Rd., Huwei Township, Yunlin County 632301, Taiwan*

ARTICLE INFO

Article History

Received 31 October 2023
Accepted 13 March 2025

Keywords

Blockchain
Water Dam
Critical Infrastructure

ABSTRACT

Ensuring the data integrity and safety of dam infrastructure is a major challenge. In recent years, numerous cyberattacks have targeted critical infrastructure, underscoring the importance of security systems. To address this challenge, we propose DamChain, a warning system designed to improve the data integrity and security of dam infrastructure based on blockchain technology. The decentralized ledger of blockchain records data in a transparent and immutable manner, which is important for ensuring the integrity of data and preventing unauthorized modification. This system aims to provide a solution that maintains the data integrity and is designed to provide a warning mechanism about water levels, improving the security and data integrity of dams.

1. Introduction

Water dams play an important role in water resource management, energy production, and flood control. Therefore, ensuring the integrity and security of dam infrastructure is important to prevent potential disasters. The 2022 cyberattack on a Ukrainian power company, resulting in data manipulation [1], demonstrates the importance of securing critical infrastructure against cyberattacks [2].

Numerous studies have explored the application of blockchain technology in various domains, including healthcare, finance, and IoT [3]. Blockchain, as a decentralized ledger, provides transparency, resilience, and immutability against unauthorized modification, making it a possible solution for critical infrastructure like dams.

In research by Liu et al., a cross-organizational non-repudiation industrial control log system based on blockchain was introduced. This system ensures the security and integrity of operation logs [4]. Another study proposed the utilization of blockchain to monitor device functioning within industrial control systems, thereby enhancing system security and stability [5]. Inspired by these studies, this paper proposes the network architecture and operational workflow of a warning system based on blockchain, contributing to the enhanced security of dam infrastructure.

Corresponding author E-mail: jsli@cans.ee.ncku.edu.tw

2. Background

2.1. *Regulatory and Policy*

Regulatory and policy frameworks provide a framework for ensuring the security, safety, and resilience of dam infrastructure. This may include rules for access controls, data protection, and incident response plans. Compliance with these regulations and policies is essential for ensuring the resilience of dam infrastructure against potential cyber threats, as well as for ensuring the safe operation of the proposed warning system based on blockchain technology.

These frameworks must also consider the importance of maintaining consistency between operational records and actual activities to ensure the reliability of dam operations. This involves establishing guidelines for recording dam operations, including water level monitoring and emergency response procedures, to ensure accuracy and compliance with regulatory

requirements. Maintaining this consistency ensures that operational decisions are based on reliable data.

If the status of dam gates displayed in the system does not match their actual physical state, it can be dangerous. For instance, the system might indicate that the gates are closed when, in fact, they are open; alternatively, the system could show the gates as open when they are actually closed, leading to potentially incorrect assumptions and actions by operators. This discrepancy can result in uncontrolled water flow, which might cause flooding downstream or put the structural integrity of the dam at risk. Such situations could lead to severe consequences.

Implementing comprehensive monitoring rules, supported by clear regulatory and policy frameworks, is important to ensure that operational records accurately reflect the true state of dam infrastructure. By establishing transparent and reasonable processes for data collection and reporting, operators can enhance the reliability and integrity of dam operations, ultimately safeguarding dam infrastructure.

2.2. *Data Integrity*

Data integrity within the dam infrastructure system is important to ensure that data remains consistent, accurate, and reliable, especially in the face of potential unauthorized access and malicious attacks. This integrity is important for sustaining the safety and effectiveness of water management, energy production, and flood control operations. Compromises to data integrity can result in incorrect decisions and operational disruptions, posing significant risks to public safety and environmental stability [6].

Ensuring data integrity is important for maintaining the security of dam infrastructure. Accurate data is essential for monitoring water levels, detecting anomalies, and predicting potential risks such as floods or structural failures. Compromised data integrity could result in incorrect assessments of risks, leading to delayed responses to emergencies.

Malicious hackers and unauthorized individuals may attempt to compromise data integrity through various mean. In addition to the risk of data being tampered with by hackers, there is also the potential threat of unauthorized modifications by internal employees. Employees may utilize their privilege to modify data for personal advantage or cover up unauthorized actions. Insider threats can be particularly challenging to detect, as these individuals often have a deep understanding of the vulnerabilities of the dam infrastructure system.

Blockchain can serve as digital evidence because it provides a secure and immutable record of operational data. This ensures that the data on the blockchain can be used as reliable digital evidence in audits, legal proceedings, and other situations where proof of authenticity and accuracy is required. The ability of blockchain to maintain a verifiable and unchangeable history of records makes it a powerful tool for preserving digital evidence.

Safeguarding data integrity is important for maintaining the security, reliability, and effectiveness of dam infrastructure operations. By implementing advanced technologies like blockchain, dam operators can ensure the data integrity of dam infrastructure in the face of potential threats [7].

3. DamChain Architecture

The system architecture utilizes blockchain technology to improve the safety and reliability of dam operations. The integration of several components within the system architecture works together to ensure the data integrity related to dam infrastructure.

3.1. *Network Architecture*

The network architecture integrates dam operations and water level monitoring with blockchain technology to improve the security and reliability of important data related to dam infrastructure. This integration is depicted in Fig. 1. The diagram illustrates a network architecture that integrates dam operations and water level monitoring with blockchain technology.

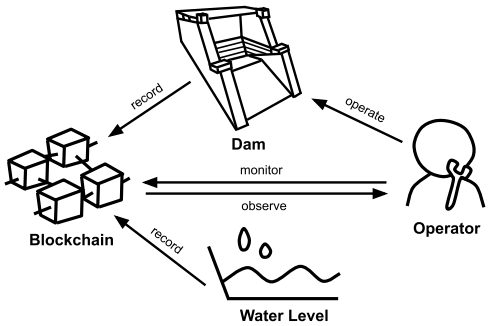

Fig. 1 Network Architecture

The dam is responsible for operating and managing water levels. The blockchain serves as a distributed database where all dam operations and water level data are recorded and stored securely. This includes water level data collected from water sensors, ensuring that operators have access to information about the dam operations and water level data. the system achieves protection against tampering by recording water levels and operational data on the blockchain, ensuring the

integrity of the important data related to dam infrastructure.

3.2. *Operational Workflow*

The operational workflow shows a comprehensive approach to managing dam operations and ensuring compliance with regulatory requirements. This process ensures that operational data are recorded and monitored, with appropriate actions taken based on predefined conditions. Fig. 2 is the operational workflow designed for managing dam operations through blockchain technology.

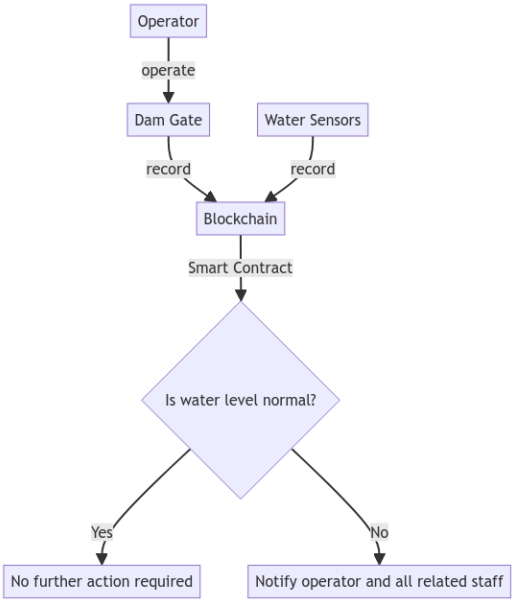

Fig. 2 Operational Workflow

The dam operator controls water flow through interaction with the dam gates. These actions are logged on the blockchain to ensure transparency and tamper resistance of operational data. The water level sensors monitor water levels and record data on the blockchain. The smart contract evaluates the recorded data to determine if water level is normal. If the water level is abnormal, the smart contract triggers a notification to the operator and all related staff, prompting them to take appropriate response to the situation.

4. Experiment

The experiment evaluated the performance of the proposed dam warning system, utilizing Geth (Go Ethereum) for blockchain implementation. The system operated on a computer with specifications listed in Table 1.

Table 1. Experiment Evironment

CPU	Intel Core i5-7500 @ 3.40 GHz
OS	Windows 10 Enterprise 64-bit
RAM	16GB

Fig. 3 shows the transaction count on the blockchain. The horizontal axis represents elapsed time, ranging from 5 seconds to 40 seconds, while the vertical axis represents transaction count, measured in transactions per 5 second. This indicates that the system, within the specified hardware and software environment, is capable of processing and recording dam operations, with an average throughput of approximately 115.575 transactions per second.

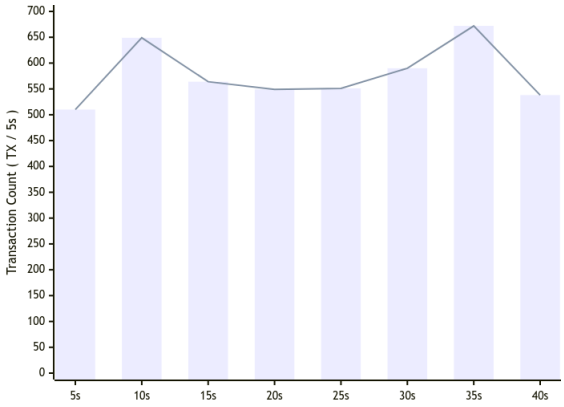

Fig. 3 Transaction Count

Fig. 4 shows the experimental results of the response times to water level alert events. The horizontal axis represents different trials or instances, numbered from 1 to 8. On the vertical axis, the response time is measured in seconds. The consistent height of the bars indicates that the response time remained relatively stable across different instances of water level alert events.

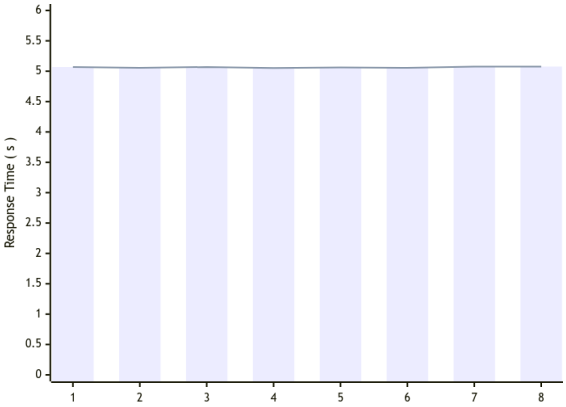

Fig. 4 Response Time

Across multiple trials, the system consistently responded to alert events with an average response time of approximately 5.064 seconds. The consistency in response time indicates the reliability of the system in addressing water level alerts promptly and efficiently. The results validate the efficacy and efficiency of the proposed dam warning system, showing its ability to provide timely responses to water level alerts.

5. Conclusion

The regulatory and policy frameworks are important for ensuring the safety of a dam. By adhering to established rules, operators can make consistent decisions that minimize potential risks. The integration of blockchain technology provides an immutable mechanism that records important operational data. offers a solution for ensuring data integrity within dam operations, ensuring that the operational data for critical infrastructure remains trustworthy, thus enhancing the overall security of the system.

The system integrates blockchain technology, network architecture, and operational workflow to create a and secure framework for critical infrastructure. The system also implements a water level alert feature, which monitors the water levels and triggers warnings when they reach predefined thresholds, further improving data integrity and dam security.

Acknowledgements

This work was supported by the National Science and Technology Council in Taiwan under contract numbers NSTC 112-2634-F-006-001-MBK and 113-2634-F-006-001-MBK.

References

1. ESET Research, "Industroyer2: Industroyer reloaded This ICS-capable malware targets a Ukrainian energy company," 2022.
2. CNN, "Russian military-linked hackers target Ukrainian power company, investigators say," 2022.
3. K. Christidis and M. Devetsikiotis,"Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292 - 2303, 2016.
4. I-H. Liu, Y.-C. Tsai, C.-F. Li and J.-S. Li, "Cross-organizational Non-repudiation Industrial Control Log," Journal of Robotics, Networking and Artificial Life, vol. 9, no. 3, pp. 240 - 244, 2022.
5. I-H. Liu, C.-H. Wu, J.-S. Li and C.-F. Li, "Utilizing Blockchain to Monitor the Functioning of Devices in Industrial Control Systems," Journal of Advances in Artificial Life Robotics, vol. 3, no. 4, pp. 205 - 208, 2023.
6. A. Parvizimosaed, H. Azad, D. Amyot and J. Mylopoulos, "Protection against Ransomware in Industrial Control Systems through Decentralization using Blockchain," 2023 20th Annual International Conference on Privacy, Security and Trust (PST), Copenhagen, Denmark, 21-23, Aug., 2023.
7. Y. Shah and S. Sengupta, "A survey on Classification of Cyber-attacks on IoT and IIoT devices," 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 28-31, Oct., 2020.

Authors Introduction

Dr. I-Hsien Liu

He is an assistant professor in Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his Ph.D. in 2015 in Computer and Communication Engineering from the National Cheng Kung University. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU).

Mr. YingCheng Wu

He is acquiring a master's degree in the Department of Electrical Engineering/Institute of Computer and Communication Engineering, National Cheng Kung University, Taiwan. His interests are Cyber-Security and Blockchain.

Dr. Chu-Fen Li

She is an Associate Professor in the Department of Finance at the National Formosa University, Taiwan. She received her PhD in information management, finance and banking from the Europa-Universität Viadrina Frankfurt, Germany. Her current research interests include intelligence finance, e-commerce security, financial technology, IoT security management, etc.

Dr. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in Computer Science from the Technical University of Berlin, Germany. He is the director of Taiwan Information Security Center @ National Cheng Kung University.