Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 5, pp. 4014–4022, DOI 10.12694/scpe.v25i5.3154

RESEARCH ON CRYPTOGRAPHY-BASED DATA SECURITY AND TRUSTWORTHINESS IN DIGITAL CONSTRUCTION OF WATER RESOURCES AND HYDROPOWER

CHAO YUE*, WEI LIU†, LICHENG CHEN‡ AND CHONG ZUO§

Abstract. This study aims to strengthen data security and establish credibility using novel cryptography-based techniques in the context of the digital revolution in the water resource and hydropower development industry. Protecting sensitive data and guaranteeing the confidentiality of digital assets becomes crucial as the sector depends more and more on digital technology for communication, monitoring, and project management. The goal of this work is to create developed cryptographic protocols and structures that have been tailored to the needs of the water resources and hydropower industry. This study offers a thorough investigation into the use of cryptographic methods to tackle the difficulties presented by the digital construction surroundings in these projects. The research process combines algorithm creation, theoretical advancements, and real-world application. The efficiency and viability of the suggested cryptographic approaches in resolving trust and security issues intrinsic in digital building environments will be evaluated using actual-life scenarios and simulations. The results of this study should offer a strong basis for improving data security, reliability, and integrity in digital construction projects related to water resources and hydropower. Through the development of cryptography techniques specifically suited to this vital infrastructure industry, the research helps to build digital ecosystems that are resilient and secure, which is important for the sustainable growth of hydropower and water resources.

Key words: Cryptography, Data Security, Trustworthiness, Digital Construction, Water Resources and Hydropower

1. Introduction. Energy is crucial to the economy's ability to grow sustainably [10]. Although nuclear energy and fossil fuels are frequently used to generate electricity, they frequently cause some environmental harm due to the emissions of CO2 as well as other radioactive substances. Sustainable and alternative sources of energy have been heavily pushed in such a situation. One option for efficiently preserving the natural world is hydropower. It is seen as a component of a low-carbon economic system's energy combine, particularly for nations that are developing [20]. Hydropower, the world's most productive renewable energy resource for electricity generation, produces 71% more electrical power than other energy sources including coal, gas, and oil [13].

There are certain benefits to using hydropower to generate electricity. It is less expensive, more sustainable, and more dependable than coal, gas, or oil. There are less environmental restrictions on hydropower than on solar and wind power [23]. Hydropower now plays a larger role than it did previously since it is acknowledged as being fundamental to the production of energy [16]. Since concealed or in-conduit hydropower systems are completely incorporated into the current infrastructure, they have less of an environmental impact than conventional hydropower plants that operate in rivers [6]. Particularly, these hydropower systems capture the extra energy of water that is being utilized for purposes other than electricity production.

A geodatabase of unexplored prospective places for energy recovery at current hydro facilities in particular European towns and nations has been produced by an ongoing study [24, 5]. Building an in-conduit hydropower system could be advantageous for governmental treatment works, including wastewater amenities, and public water systems, considering their respective consequences. The author [26, 27] provided a thorough summary

*Hydropower and Water Conservancy Engineering Institute POWERCHINA HUADONG Engineering Corporation Limited, Hangzhou, Zhejiang, 311122, China (chaoyuedigital12@outlook.com)
†Hydropower and Water Conservancy Engineering Institute POWERCHINA HUADONG Engineering Corporation Limited, Hangzhou, Zhejiang, 311122, China
‡Dagu Hydropower Branch of Huadian Xizang Energy Co., Ltd., Shannan, Xizang, 856000, China
§Hydropower and Water Conservancy Engineering Institute POWERCHINA HUADONG Engineering Corporation Limited, Hangzhou, Zhejiang, 311122, China

of the advancements in in-conduit hydropower technology and their uses. In [22], actual case studies of small hydro turbines incorporated into drinking water and wastewater networks were provided together with a succinct technical explanation. Numerous nations have evaluated the potential for hydropower, including the feasibility of putting turbines in water and wastewater infrastructure from a technical and financial standpoint.

Turbine installation is typically ideal near wastewater treatment outlets because of the steady and enough water flow. The WWTP process involves constant monitoring of the variables needed to choose hydro turbines, like head and flow. As such, monitoring the turbine's functioning can be rather simple [4]. On the other hand, low- or ultralow-head plants may face a problem if the tailwater effect is overlooked. The head is reduced at most sites during a flood period because the tailwater level at the outfall rises greater than the level upstream of the intake, depending on the receiving water body (such as a river). Nevertheless, the literature hardly ever discusses these situations.

The motivation for this research emerges from the critical need to enhance data security and establish a foundation of trust within the rapidly digitising landscape of the water resources and hydropower development industry. As this sector increasingly relies on digital technologies for essential operations such as communication, monitoring, and project management, the protection of sensitive data and the confidentiality of digital assets become paramount. The advent of the digital revolution in this field presents immense opportunities and significant challenges, particularly regarding safeguarding against cyber threats and ensuring the integrity of digital construction environments.

This study is driven by the recognition that conventional cryptographic protocols and security measures may not fully address the unique complexities and requirements of the water resources and hydropower industry. These projects are characterized by their extensive scale, long duration, and the critical nature of their infrastructure, which necessitates a bespoke approach to data security. The research aims to develop and refine cryptographic techniques specifically tailored to meet these industry-specific needs, providing robust protection for digital assets and sensitive information.

The main contribution of the proposed method is given below:

1. Creation of customized cryptography protocols intended to handle the trust and security issues that arise during the digital construction lifespan of hydropower and water resource projects.
2. The security and reliability of vital project information are guaranteed by these protocols, which offer a framework for protecting sensitive data throughout transfer, storage spaces. and retrieval.
3. Scaling and efficiency improvements for cryptographic solutions while considering the special requirements of large-scale water resource and hydropower projects involving a variety of stakeholders.
4. By balancing strong security measures with effective data processing, the research helps build cryptographic algorithms that are useful in real-world construction circumstances.

The rest of our research article is written as follows: Section 2 discusses the related work on various classification of brain image processing and methodData Security and Trustworthiness in Digital Construction of Water Resources and Hydropower s. Section 3 shows the algorithm process and general working methodology of proposed work. Section 4 evaluates the implementation and results of the proposed method. Section 5 concludes the work and discusses the result evaluation.

2. Related Works. Cyberattacks are online activities that try to break into the computer networks of people or organizations with the intention of causing damage or interrupting operations. These assaults may target various objectives, such as stealing sensitive data or jeopardizing data integrity [2]. For energy and electricity systems to operate securely and dependably, sufficient protection layers must be developed for a CPS. Nonetheless, the electricity sector has seen a rise in cyberattack efforts in recent years. Approximately 800 cyberattacks have been reported in the energy sector since the 1980s [3].

A thorough review of turbines suitable for concealed hydro and in-conduit hydropower was provided in [21, 17], with a focus on current developments in the field of turbine technology. Novel technological approaches have been put forth that enhance traditional turbines with stronger designs, increased efficiency, and potentially cheaper costs [14]. However, while more recent or developing technologies present creative methods for in-conduit hydro generation, they may not necessarily be the most economical option [19]. The comparison of equipment costs is complex because of the different sites and turbines. However, modular structures may have higher hydromechanical and electric running costs than traditional turbines, even though their building and

installation expenses may be lower [12, 11].

Low-cost engines, such as pumps as turbines (PaTs), are recommended because traditional hydro turbine technologies aren't always competitive in the market. These are regular pumps that have had their flow direction reversed so that they can be used as turbines. PaTs have been the subject of research for almost a century, and their use in small- and micro-hydropower is still significant today [7, 8, 25]. PaTs are typically employed at locations with greater head counts; the literature hardly ever discusses low-head application experience.

Most importantly, tools that assist water and wastewater providers in determining whether establishing hydropower facilities is both technically and financially feasible should be developed [1, 28]. Evaluation instruments must be as simple to use and economical as feasible because the majority of in-conduit or hidden hydro systems have comparatively limited capacities and, as a result, require a highly expensive feasibility study. For small developers, these needs are not met by the tools that are now available [15]. It has been suggested that conduit projects be evaluated using a few engineering design tools. However, these have not yet been used in more comprehensive analyses. To be sure, the US-developed tools are partly to blame for some exceptions [18, 9]. These are free-to-use tools that work with widely accessible spreadsheet software.

Given the extensive geographical spread of water resources and hydropower infrastructure, cryptographic protocols must be scalable across large distributed networks. This might involve optimizing encryption algorithms for low-latency operations and ensuring they can handle the high volume of data generated by IoT devices and sensors without compromising performance. Many operations within the sector rely on real-time data for monitoring and control. Cryptographic protocols can be modified to support efficient real-time encryption and decryption processes, enabling secure yet timely data transmission crucial for operational decision-making. Adapting cryptographic protocols to be compatible with existing industrial control systems (ICS) and operational technology (OT) used in the sector. This may require developing lightweight cryptographic solutions that can be implemented on legacy systems without significant hardware upgrades. With the increase in remote monitoring and management of hydropower plants, cryptographic protocols need to ensure secure remote access. This could involve adapting protocols to provide robust authentication and secure communication channels for remote users, preventing unauthorized access and ensuring data integrity.

3. Proposed Methodology. The proposed method uses Cryptographic techniques for Data Security and Trustworthiness in the Digital Construction of Water Resources and Hydropower. Create protocols for encryption with data transfer, storage, and access control specifically suited to the digital building lifecycle. Create protocols that handle issues including permission procedures, secure interaction with stakeholders, and data tampering prevention. The purpose of this proposed technique is to improve data security and reliability in the digital design of hydropower and water resource projects by exploring and carrying out cryptography-based technologies in an organised and rigorous manner. In figure 3.1 shows the architecture of the proposed method.

The water resource and hydropower industry faces unique cryptographic needs and challenges stemming from its critical infrastructure status, the complexity of its operational environments, and the increasing digitization of its processes. Addressing these challenges is crucial for ensuring the security, reliability, and resilience of these essential services. Here are some of the specific cryptographic needs and challenges in this industry: 1. The industry relies heavily on real-time data for monitoring water levels, flow rates, and power generation metrics. Cryptographic solutions must provide real-time encryption and decryption of data streams without introducing significant latency, which could impact operational efficiency and safety. 2. Water resource and hydropower systems often encompass extensive geographical areas with multiple sites and installations connected via distributed networks. Cryptographic protocols must be scalable and flexible enough to secure communications across these vast and varied landscapes. 3. Given its importance to national security and the economy, the industry is a potential target for state-sponsored and sophisticated cyber-attacks, including Advanced Persistent Threats (APTs). Cryptographic measures must be robust enough to protect against such threats, ensuring the integrity and availability of control systems.

3.1. Homomorphic Encryption Techniques. These allow calculations to be performed on encrypted data without requiring decryption. Homomorphic encryption might be useful for secure computing on sensitive data without exposing it during processing in water resources and hydropower.

HE is a type of encryption that enables computation between plaintexts that are concealed in cipher-text. Another cipher-text with the correct plaintext-to-plaintext calculation output can be the result of the

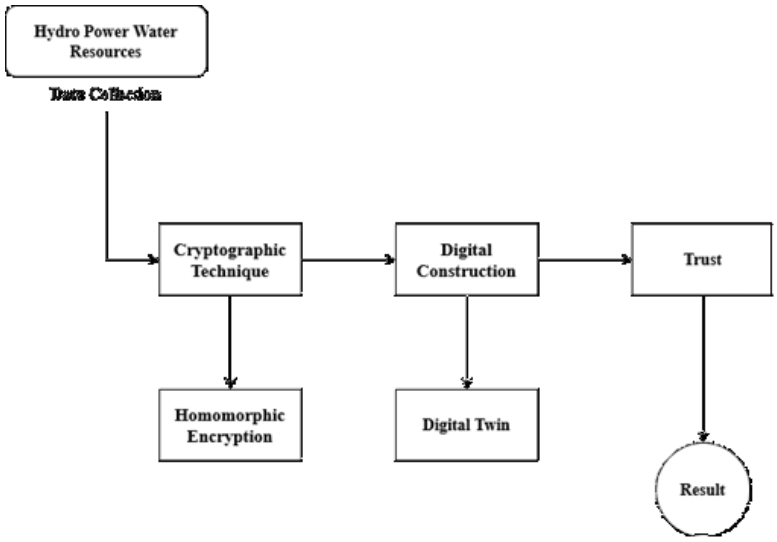

Fig. 3.1: Architecture of Proposed method

computation in HE. Since the ciphertext completely encloses the plaintext and data encryption only permits the decryption and encryption procedures, the hidden plaintext within the ciphertext cannot be altered using conventional encryption techniques. Therefore, to obtain the plaintexts, which can be utilized to perform operations on the original message contained in the cipher-texts, the cipher-texts must be decoded.

By enabling secure computations on encrypted data, HE reduces the need for complex data protection measures that might otherwise slow down processing or increase operational costs. This can lead to more efficient system operations and reduced overhead for security. As cyber threats evolve, the ability to compute on encrypted data provides a forward-looking approach to data security, ensuring that the sector is prepared for emerging challenges and can safeguard sensitive information against future vulnerabilities.

3.2. Digital Twin-based Digital Construction of Water Resources and Hydropower. The preparation, design, building, and administration of infrastructure connected to water resources and hydropower generation are improved using cutting-edge digital technologies and data-driven approaches in digital construction projects. With the creation and management of water-related projects, this innovative strategy makes use of digital tools to streamline procedures, boost productivity, and guarantee sustainability.

A virtual copy of a real object, system, or procedure is called a digital twin. Digital twins can simulate a project's whole lifecycle in the context of hydropower and water resources, offering real-time insights and assisting in improved decision-making. The use of digital twins makes it possible to simulate, analyse, and monitor hydropower facilities, dams, and water systems. They support the long-term resilience of infrastructure, performance optimization, and maintenance demand prediction.

Making a thorough 3D model or depiction of the real object or system is the first step in creating a digital twin. The digital twin is built on top of this model. When it comes to water resources and hydropower, the physical assets—like dams, water treatment facilities, or hydropower plants—as well as their components, dimensions, and functional features are digitally modelled.

3.3. rustworthiness for water resources and Hydropower. The reliability, integrity, and security of the systems, procedures, and data involved in controlling and producing electricity from water resources are referred to as trustworthy in the context of hydropower plants and water resources. Establishing credibility is essential to guarantee the security, longevity, and effective functioning of water-related infrastructure.

Guaranteeing the precision and dependability of information gathered from sensors, surveillance tools, and additional sources in water infrastructure. To make well-informed decisions about hydropower generation, dam safety, and water flow, one must have faith in the accuracy of data. To keep data accurate, regular validation and

Algorithm 1 Homomorphic Encryption

Input: Public key, KW
Output: verifying the result
initialize keywords KW into T0;
select key K_{se} for P_{R_f} // K_{se} is Key search
select K_x, K_i, K_z for $P_{R_f} F_p$
KeF(K_{se},W)
for i **do**d $\in$ DB(W) d_0 do
    counter C1
    evaluate $X_{i_d} \leftarrow F_p\left(K_i, i_d\right), Z \leftarrow F_p\ \left(K_z, w||C\right)$;

$$Y \leftarrow X_{id_z} - 1e \leftarrow E_{n_c}(K_e, i_d);$$

$$Xt_{a_g} \leftarrow gF_p\left(K_x, w\right) X_{i_d} and\ X_{Se_t} \leftarrow\ X_{Se_t}\ Ux_{ta_g};$$

    append (y,e) to t and $C \leftarrow C + 1$;
    T[w] $\leftarrow t$;
end for
return $E_{D_B}, K = (K_{se}, K_x, K_i, K_z, K_t)$;
generating a token $\left(q\left('w\right), K\right)$;
evaluate $stag \leftarrow T_S et.Get\gamma ag(K_t, w_1)$;
The server receives data from the user.
for C **do**=1,2,…. Until the server halts do
    for i **do**=2,…,n do
        $xt_{o_{k_{e_n|C|}}} \leftarrow gF_p(K_z, w1||C)F_p(K_x, w_i)$;
    end for
    $xt_{o_{k_{e_n|C|}}} \leftarrow (xt_{o_{k_{e_n|C,2|}}}, \ldots.., x_{token|C,n|})$;
end for
$Tokq \leftarrow (s_{ta_g}, x_{to_{k_{e_n}}})$;
return T okq;
end

verification procedures are necessary. Building and upholding technology that is resilient to calamities, severe weather, and other possible disruptions. The incorporation of resilience into water infrastructure guarantees its capacity to operate in challenging circumstances, mitigating the likelihood of malfunctions, and enhancing its enduring reliability.

Keeping lines of communication open and honest with all parties involved, such as the public, neighbours, and regulatory bodies. By giving accurate information about the workings, safety precautions, and possible effects of water infrastructure projects, open communication promotes healthy relationships with neighbours and fosters trust.

4. Result Analysis. Numerous writers have created geodatabases and utilized geographic information (GIS data) to find possible hydro sites in water distribution systems. Spatial databases, or high-resolution digital elevation or terrain models (DEMs), are available in many nations. Along with the Shuttle Radar Topography Mission (SRTM) DEMs from the United States Geological Survey, global terrain data from Google Earth or other platforms can also be used, but they should be used cautiously—that is, only for the initial assessment of SHP locations and not for flat terrains or low-lying countries and areas with a low vertical resolution in geography.

The proposed method uses parameter metrics such as accuracy, precision, recall and f1-score for hydropower water resources.

Accuracy is a crucial criterion that relates to the precision and correctness of numerous processes, data, and outcomes in the context of digital creation of hydropower and water resources. the accuracy of spatial data utilized in the planning and design stages, such as maps, surveys, and geographical information systems (GIS). Precise geographic information guarantees that the project site's physical attributes are accurately depicted,

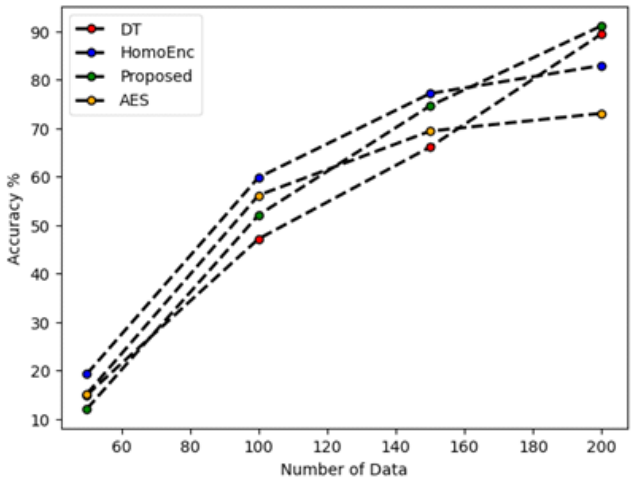

Fig. 4.1: Accuracy

reducing mistakes in both design and construction.

The accuracy of quality assurance procedures and examinations conducted both during and following construction. Precise quality control and inspections guarantee that constructed pieces fulfil the intended quality standards and help to ensure compliance with industry standards, legal requirements, and project specifications. the accuracy of the information kept in asset management systems, which are used to keep an eye on and repair water infrastructure. For efficient maintenance scheduling, preparation, and management throughout their lifecycle to ensure the durability and dependability of water-related resources, reliable asset data is crucial. In figure 4.1 shows the accuracy of proposed method.

When discussing digital construction for hydropower and water resource projects, precision pertains to the precision and dependability of the algorithm or system in recognizing and detecting elements or features within digital data. When it comes to activities such as object detection, where the objective is to reduce false positives and make sure that features recognized are relevant to the construction process, precision is an important parameter.

The ratio of true positives to the total of true positives and false positives is used to compute precision. This refers to precisely recognizing and finding pertinent objects or elements inside the digital model of the infrastructure or building site in the context of digital construction. To reduce false positives, which might influence the construction process and result in wrong judgments, high precision is necessary. It guarantees the reliability and applicability of the features found. In figure 4.2 shows the evaluation of Precision.

"Recall" generally refers to a measurement of performance used to assess the efficacy of methods or systems in the context of digital construction of hydropower and water resource projects, particularly in activities involving object detection or recognition. Recall, which is sometimes referred to as sensitivity or true positive rate, quantifies a system's capacity to accurately identify every pertinent case among all actual occurrences. In digital construction, recall evaluation is an element of an iterative process. Based on the feedback from memory evaluations, the system can be modified and fine-tuned to increase its capacity to recognize and recall pertinent aspects or abnormalities in the building procedure. In figure 4.3 shows the evaluation of Recall.

A metric called the F1-score, sometimes referred to as the F1 measure or F1-value, combines recall and precision into a single number. It is especially helpful in situations when there is an unequal distribution of classes, and it is important to consider both false positives and false negatives. The F1-score can be utilized in the digital design of hydropower and water resource projects to assess how well models or algorithms perform in tasks like object detection, image categorization, or predictive maintenance.

Evaluating the precision of algorithms used to detect things in photos, such as tracking infrastructure elements or spotting anomalies. Assessing the effectiveness of models that forecast equipment breakdowns

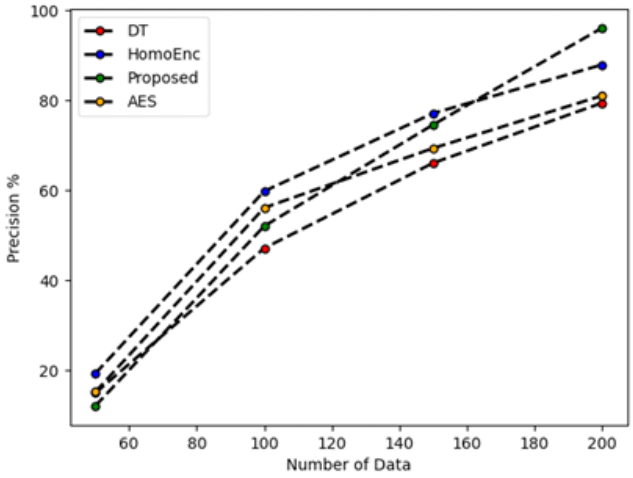

Fig. 4.2: Precision

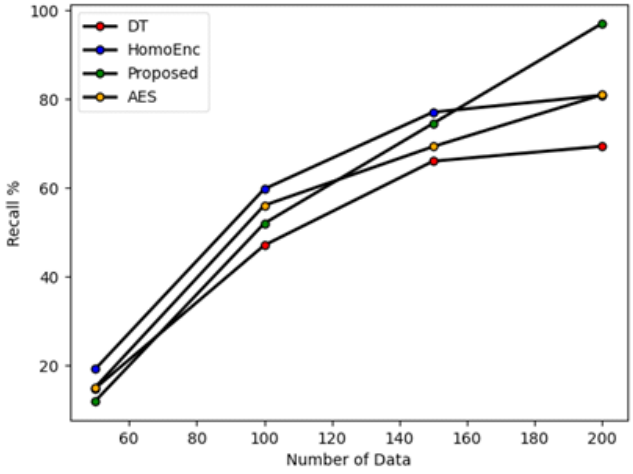

Fig. 4.3: Recall

or the need for maintenance to guarantee the dependability of hydropower facilities. Evaluating how well models categorize photos of building sites or the state of infrastructure connected to water. It is imperative to consider the goals of the work and the relative significance of recall and precision considering the application requirements when interpreting the F1-score. A balance between recall and precision may be more acceptable in certain situations, while a greater emphasis on precision may be preferred in others. In figure 4.4 shows the evaluation of F1-score.

5. Conclusion. The objective of this research is to enhance data security and establish credibility in the context of the digital revolution in the water resource and hydropower development industry by utilizing innovative cryptography-based techniques. As the industry grows more and more reliant on digital technology for project management, monitoring, and communication, safeguarding sensitive data and ensuring the confidentiality of digital assets becomes essential. This initiative aims to design cryptographic structures and protocols specifically suited to the demands of the hydropower and water resources sectors. This paper provides a com-

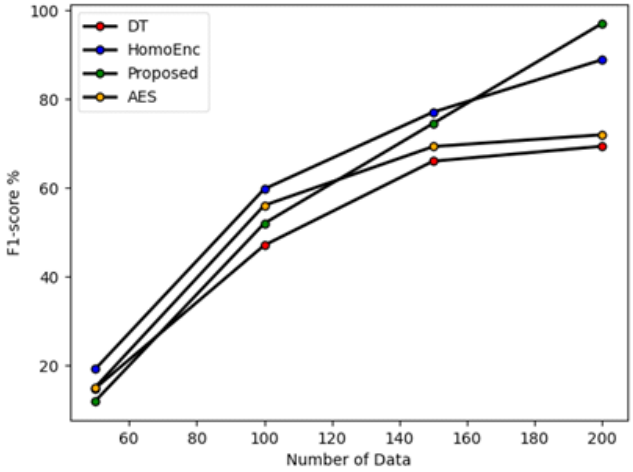

Fig. 4.4: F1-score

prehensive analysis of the application of cryptographic techniques to address the challenges posed by the digital building environment in these projects. The development of algorithms, theoretical breakthroughs, and practical implementation are all combined in the research process. Using real-world examples and simulations, the effectiveness and practicality of the proposed cryptographic techniques in addressing trust and security concerns inherent in digital building environments will be assessed. The findings of this research should provide a solid foundation for enhancing data security, dependability, and integrity in digital construction projects involving hydropower and water resources. By creating cryptographic methods tailored to this essential infrastructure sector, the research contributes to the construction of robust and secure digital ecosystems, which is necessary for the long-term development of hydropower and water resources.

Acknowledgement. This work was sponsored in part by National Natural Science Foundation of China (2345678)

REFERENCES

[1] M. Abdelmalak, V. Venkataramanan, and R. Macwan, *A survey of cyber-physical power system modeling methods for future energy systems*, IEEE Access, (2022).
[2] E. Ahmadian, C. Bingham, A. Elnokaly, B. Sodagar, and I. Verhaert, *Impact of climate change and technological innovation on the energy performance and built form of future cities*, Energies, 15 (2022), p. 8592.
[3] E. Ahmadian, H. Byrd, B. Sodagar, S. Matthewman, C. Kenney, and G. Mills, *Energy and the form of cities: the counterintuitive impact of disruptive technologies*, Architectural science review, 62 (2019), pp. 145–151.
[4] E. Ahmadian, B. Sodagar, C. Bingham, A. Elnokaly, and G. Mills, *Effect of urban built form and density on building energy performance in temperate climates*, Energy and Buildings, 236 (2021), p. 110762.
[5] W. Ascher, *Rescuing responsible hydropower projects*, Energy Policy, 150 (2021), p. 112092.
[6] N. Diaz-Elsayed, N. Rezaei, A. Ndiaye, and Q. Zhang, *Trends in the environmental and economic sustainability of wastewater-based resource recovery: A review*, Journal of Cleaner Production, 265 (2020), p. 121598.
[7] D. Du, M. Zhu, X. Li, M. Fei, S. Bu, L. Wu, and K. Li, *A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems*, Journal of Modern Power Systems and Clean Energy, (2022).
[8] W. Duo, M. Zhou, and A. Abusorrah, *A survey of cyber attacks on cyber physical systems: Recent advances and challenges*, IEEE/CAA Journal of Automatica Sinica, 9 (2022), pp. 784–800.
[9] A. Fausto, G. B. Gaggero, F. Patrone, P. Girdinio, and M. Marchese, *Toward the integration of cyber and physical security monitoring systems for critical infrastructures*, Sensors, 21 (2021), p. 6970.
[10] Y. Y. Ghadi, D. B. Talpur, T. Mazhar, H. M. Irfan, U. A. Salaria, S. Hanif, T. Shahzad, and H. Hamam, *Enhancing smart grid cybersecurity: A comprehensive analysis of attacks, defenses, and innovative ai-blockchain solutions*, (2023).
[11] S. He, Y. Zhou, X. Lv, and W. Chen, *Detection method for tolerable false data injection attack based on deep learning framework*, in 2020 Chinese Automation Congress (CAC), IEEE, 2020, pp. 6717–6721.

[12] S. Karamdel, X. Liang, S. O. Faried, and M. Mitolo, *Optimization models in cyber-physical power systems: A review*, IEEE Access, (2022).
[13] X. Lei, *Research on development and utilization of hydropower in myanmar*, Energy Reports, 8 (2022), pp. 16–21.
[14] M. Lezzi, M. Lazoi, and A. Corallo, *Cybersecurity for industry 4.0 in the current literature: A reference framework*, Computers in Industry, 103 (2018), pp. 97–110.
[15] J. Liu, W. Zhang, T. Ma, Z. Tang, Y. Xie, W. Gui, and J. P. Niyoyita, *Toward security monitoring of industrial cyber-physical systems via hierarchically distributed intrusion detection*, Expert Systems with Applications, 158 (2020), p. 113578.
[16] R. Llácer-Iglesias, J. M. Pérez, J. R. Satorre-Aznar, P. A. López-Jiménez, and M. Pérez-Sánchez, *Energy recovery in wastewater treatment systems through hydraulic micro-machinery. case study*, Journal of Applied Research in Technology & Engineering, 1 (2020), pp. 15–21.
[17] F. Longo, A. Padovano, G. Aiello, C. Fusto, and A. Certa, *How 5g-based industrial iot is transforming human-centered smart factories: a quality of experience model for operator 4.0 applications*, IFAC-PapersOnLine, 54 (2021), pp. 255–262.
[18] D. L. Marino, C. S. Wickramasinghe, B. Tsouvalas, C. Rieger, and M. Manic, *Data-driven correlation of cyber and physical anomalies for holistic system health monitoring*, IEEE Access, 9 (2021), pp. 163138–163150.
[19] E. M. Navarro, A. N. R. Álvarez, and F. I. S. Anguiano, *A new telesurgery generation supported by 5g technology: benefits and future trends*, Procedia Computer Science, 200 (2022), pp. 31–38.
[20] P. Punys and L. Jurevičius, *Assessment of hydropower potential in wastewater systems and application in a lowland country, lithuania*, Energies, 15 (2022), p. 5173.
[21] D. A. Pustokhin, I. V. Pustokhina, P. Rani, V. Kansal, M. Elhoseny, G. P. Joshi, and K. Shankar, *Optimal deep learning approaches and healthcare big data analytics for mobile networks toward 5g*, Computers and Electrical Engineering, 95 (2021), p. 107376.
[22] A. Raymakers, C. Sue-Chue-Lam, V. Haldane, A. Cooper-Reed, and D. Toccalino, *Climate change, sustainability, and health services research*, Health Policy and Technology, 12 (2023), p. 100694.
[23] L. F. Ribas Monteiro, Y. R. Rodrigues, and A. Zambroni de Souza, *Cybersecurity in cyber–physical power systems*, Energies, 16 (2023), p. 4556.
[24] M. M. M. Saw and L. Ji-Qing, *Review on hydropower in myanmar*, Applied Water Science, 9 (2019), pp. 1–7.
[25] S. Surya, M. K. Srinivasan, and S. Williamson, *Technological perspective of cyber secure smart inverters used in power distribution system: State of the art review*, Applied Sciences, 11 (2021), p. 8780.
[26] S. Tang, J. Chen, P. Sun, Y. Li, P. Yu, and E. Chen, *Current and future hydropower development in southeast asia countries (malaysia, indonesia, thailand and myanmar)*, Energy Policy, 129 (2019), pp. 239–249.
[27] Y. Tian, F. Zhang, Z. Yuan, Z. Che, and N. Zafetti, *Assessment power generation potential of small hydropower plants using gis software*, Energy Reports, 6 (2020), pp. 1393–1404.
[28] J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, *Cyber-physical systems security: Limitations, issues and future trends*, Microprocessors and microsystems, 77 (2020), p. 103201.

Edited by: Rajanikanth Aluvalu
Special issue on: Evolutionary Computing for AI-Driven Security and Privacy: Advancing the state-of-the-art applications
Received: Jan 6, 2024
Accepted: Feb 9, 2024