Academic Journal of Science and Technology
ISSN: 2771-3032 | Vol. 11, No. 2, 2024

Review on Verifiable Outsourcing of Industrial Internet Data in Securely Shared

Yafeng Wang, Qingtao Wu

Henan University of Science and Technology, Luoyang 471000, China

Abstract: With the rapid development of information technology, industrial Internet has also entered a rapid development stage. As cloud servers have huge storage space as well as powerful computing power, more and more resource-constrained factories outsource their data to cloud servers for computation and storage to reduce the burden of data owners. Industrial data contains information about industrially produced products, and the high value of such information attracts attacks from illegal users, which may lead to data leakage. In addition, cloud servers are not fully trustworthy; therefore, it is important to ensure the security and correctness of industrial Internet data during outsourced computation and storage for the healthy development of the industrial Internet. In this paper, we explore technical solutions to guarantee the security and correctness of industrial Internet data when outsourcing computation, to achieve the privacy protection of industrial Internet data.

Keywords: Industrial Internet Data; Outsourced Computing; Cloud Servers; Verifiable.

1. Introduction

Driven by Internet + mass innovation, the development of China's Internet industry has made remarkable progress, and industrial Internet [1] has also entered a rapid development stage. With the gradual extension of information technology to the industrial scene, the degree of digitization of the industrial production process [2] has also been gradually increased, the barriers between the real environment and the cyberspace have been broken, and the data, as an important part of the cyberspace, is also closely related to the industrial production process [3]. Among them, cloud factory [4] online manufacturing service platform is the benchmark product of the combination of Internet technology and industrial manufacturing innovation. Therefore, data sharing will become an important part of realizing the vision of field-wide and industry-wide connectivity proposed by the Industrial Internet. However, due to the obvious differences in the production sectors, industries, and technical standards to which Industrial Internet participants belong, and the data sharing under the Industrial Internet environment is a cross-domain circulation and sharing process involving industrial subjects from different fields and industries [5], which makes the raw data closely related to industrial production become the basis of data sharing. At the same time, because these data can objectively reflect the quality of products, production processes and techniques [6], they should also be regarded as an important category of privacy data.

With the rapid development of the industrial Internet, more and more scholars have begun to pay attention to the privacy data protection issues involved [7,8]. The sharing of data through the Internet enables cooperating factories and enterprises to access information such as customers' needs for products and product specifications, including a large amount of sensitive data such as introductions of different models of products, drawings with different precision, and production processes. As a product may be completed by multiple factories in co-operation, data sharing can help multiple factories to access the data as needed. However, data sharing is not absolutely safe, and if shared data is compromised, it can cause significant economic as well as reputational damage to the factory. In recent years, many data breaches have occurred around the globe [9,10], and the manufacturing industry has become a high incidence area for data breaches. Surveys have shown that in 2017 alone, there were more than 600 data privacy breaches in the global manufacturing industry, involving a large amount of sensitive data such as production processes and customer information. For example, hackers had invaded the vehicle financing department of Mazda's Canadian division, and a large amount of customer information was leaked. In 2018, sensitive data of Volkswagen, Tesla and other automobile companies were leaked. It can be seen that information leaks occur frequently, and data protection in the context of smart manufacturing cloud factories is particularly important. Therefore, how to protect the privacy of data in the context of smart manufacturing cloud factory is the main issue we should study at present.

Therefore, the data to be shared should be encrypted before data sharing [11]. However, resource-constrained factories and enterprises can hardly afford the complicated encryption calculation [12], so they must outsource the encryption operation of data to the cloud server for calculation. However, cloud servers are not completely trustworthy, in order to ensure the normal operation of smart manufacturing cloud factories, how to ensure the data security as well as data correctness when outsourcing the data calculation is the main issue that should be researched at present.

2. Correlation Technique

This section describes some of the techniques involved in ensuring the security and correctness of industrial Internet data computation in resource-constrained environments while reducing the burden on data owners.

2.1. Encryption

Encryption algorithms can be classified into symmetric encryption algorithms and asymmetric encryption algorithms. In symmetric encryption algorithm, the encryption method of single-key cryptosystem is used, and the same key is used to complete the encryption and decryption of data. Its encryption speed is fast and encryption efficiency is engaged, but

security is low. Asymmetric encryption, also known as public key encryption, uses a pair of keys (i.e., public key and private key) to complete the encryption and decryption, using the public key to encrypt the data and the private key to decrypt the ciphertext. Asymmetric encryption is more secure, but encryption and decryption are less efficient. The common asymmetric encryption algorithms are attribute-based encryption and has encryption. For the first time in the literature [13], a system to achieve sophisticated access control to encrypted data is proposed as ciphertext policy attribute-based encryption. Using this technique, encrypted data can be secured even if the third-party storage server is untrustworthy. Literature [14] proposes an efficient multi-key searchable encryption scheme that supports fine-grained access control and keyword search. The scheme is more flexible than the existing multi-key searchable encryption schemes in terms of control policy and keyword expression capability. Meanwhile, the scheme is also resistant to keyword guessing attacks.

2.2. Access Control

In order to prevent malicious users from violating data privacy in industrial internet, all users are required to satisfy the access policy set by the data owner every time they access the data. Literature [15] developed a ciphertext policy based encryption method for cloud storage. In this method, they enhance the security and privacy of user data by hiding the access policy. Then, a constant size ciphertext is generated to reduce the storage overhead. Moreover, a secure fine-grained access control system is developed using this approach. Literature [16] proposes a new encryption scheme based on ciphertext policy attributes. This approach uses fog computing to outsource the most laborious decryption operations to the fog nodes and partially decrypts the data using a primitive and efficient chaining architecture. In addition, erroneous attributes are introduced to keep the access policy private and allow users within the same group to combine their attributes to access the data while satisfying the access policy. Experiments and security analysis show that the scheme is secure and effective.

2.3. Outsourcing Computing

In order to secure the secure sharing of industrial Internet data, resource-constrained factories and enterprises can hardly afford the complicated encryption computation, so they have to outsource the encryption and decryption operations of data to cloud servers for computation. Literature [17] proposes an attribute-based encryption scheme in which all computations are outsourced to a third-party server, including computations in the encryption phase, key generation phase, and decryption phase, but the design of outsourced encryption fails to reduce the trust requirement of the outsourced cloud server. Literature [18] proposes a scheme for outsourcing the computation of ABE decryption. The scheme reduces the decryption computation overhead of the data user by transferring the complex bilinear pairing operation during decryption to the cloud server. Literature [19] constructed an efficient ciphertext policy attribute-based encryption scheme by outsourcing encryption and decryption. In their approach, both fully untrustworthy and semi-trustworthy models are used, using which the encryption and decryption cost of the user can be reduced.

2.4. Blockchain

Blockchain, as an open decentralized distributed ledger with the characteristics of multi-party maintenance, decentralization, data non-tampering, traceability, non-counterfeiting, and programmability [20,21], can help to solve the privacy problem in the process of industrial internet data sharing, open up the data silos, and provide a platform for the secure sharing of industrial internet data to generate permanent and irreversible records. Clear data ownership and effective prevention of data leakage. Compared with centralized architecture, blockchain can avoid security risks caused by single point of failure or data leakage, thus ensuring data integrity and not being tampered with. Literature [22] proposes a data privacy protection scheme for cross-side blockchain networks, which encrypts the on-chain data using a privacy-preserving technique of full homomorphic encryption to ensure the availability and invisibility of the on-chain private data.

2.5. Digital Signature

Digital signatures are commonly used to ensure the integrity of information transmission, authentication of the sender, and to prevent the occurrence of repudiation in transactions. Literature [23] proposes a verifiable outsourced ABE scheme based on edge servers and fog nodes, where the edge servers are fully responsible for the encryption of the ABE, while the fog nodes assist the data users in decrypting the data accordingly. In addition, the data obtained from the fog node decryption is verified using a data signature method to ensure the correctness of the obtained results.

3. Conclusion and Prospect

In the Industrial Internet, the use of emerging technologies has become a trend in smart industrial production. In industrial production, industrial orders have needs such as remote signing, so it is necessary to achieve secure sharing of industrial data among different factories and enterprises. When sharing data, people are increasingly concerned about whether their private data is under attack and whether their privacy is compromised. In order to ensure secure data sharing in resource-constrained environments, outsourced computing solutions have become an important technological tool to alleviate the pressure on data owners. However, when storing data encrypted to cloud servers, data signatures have become the most common method to determine whether cloud servers are correctly computed or not, and ensuring security and correctness when sharing data in resource-constrained environments is the focus of this research paper.

So far, although there are many effective solutions for secure sharing, there is still a need to explore more efficient methods with the rapid development of the Industrial Internet and the continuous improvement of technological means. Although the secure sharing methods for industrial Internet data discussed in this paper have achieved some results, further research on secure sharing of industrial Internet data is still necessary in the future.

Acknowledgments

This work was supported in part by the Key Technologies R & D Program of Henan Province under Grant No. 222102210080 and 242102211024, in part by the Longmen Laboratory Frontier Exploration Project of Henan Province under Grant No. MQYTSKT035, in part by the joint Funds

for Science and Technology Research and Development Plan of Henan Province under Grant No. 222103810031.

References

[1] Bao Y, Zhang X, Wang C, et al. Further expansion from smart manufacturing system to social smart manufacturing system based on industrial internet [J]. Computers Industrial Engineering, 2024, 191110119-.

[2] Dück J. Digitalization of production systems: getting smart while keeping out of harm's way? [J]. Automotive Industries, 2021, 200(1): 82-84.

[3] Pankesh P, Intizar M A, Amit S. From raw data to smart manufacturing: AI and semantic web of things for industry 4.0 [J]. IEEE Intelligent Systems, 2018, 33(4): 79-86.

[4] Huo Y, Xiong J, Guo Z, et al. A collaboration approach for cloud factories based on Kuhn–Munkras algorithm [J]. International Journal of Computer Integrated Manufacturing, 2022, 35(9): 972-988.

[5] Rajesh B, S. J, N. S. Security and privacy preservation using constructive hierarchical data-sharing approach in cloud environment [J]. Information Security Journal: A Global Perspective, 2024, 33(1): 1-15.

[6] Gao Z, Xu F, Zhou C, et al. Critical procedure identification method considering the key quality characteristics of the product manufacturing process [J]. Processes, 2022, 10(7): 1343-1343.

[7] Hui H, Zhou C, Xu S, et al. A novel secure data transmission scheme in industrial internet of things [J]. China Communications, 2020,17(1):73-88.

[8] Amalie D, Michael P, Stephanie C, et al. Differential privacy for public health data: An innovative tool to optimize information sharing while protecting data confidentiality [J]. Patterns, 2021, 2(12): 100366-100366.

[9] Ermetic: Nearly 100% of Companies Experienced a Cloud Data Breach in Past 18 Months [J]. Wireless News, 2021.

[10] In L. An analysis of data breaches in the U.S. healthcare industry: diversity, trends, and risk profiling [J]. Information Security Journal: A Global Perspective, 2022, 31(3): 346-358.

[11] Zhao Z, Xu X. Research on the application of computer data encryption technology in cloud security [J]. International Journal of Engineering and Technology, 2022.

[12] Madhu G, Kumar V P. A survey and analysis of different lightweight block cipher techniques for resource-constrained devices [J]. International Journal of Electronic Security and Digital Forensics, 2022, 14(1): 96-110.

[13] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C]. 2007 IEEE symposium on security and privacy (SP'07). IEEE, 2007: 321-334.

[14] Li W, Xu L, Wen Y, et al. Conjunctive Multi-key searchable encryption with attribute-based access control for EHR systems [J]. Computer Standards Interfaces, 2021.

[15] Chinnasamy P, Deepalakshmi P, Dutta A K, et al. Ciphertext-policy attribute-based encryption for cloud storage: Toward data privacy and authentication in AI-enabled IoT system [J]. Mathematics, 2021, 10(1): 68.

[16] Saidi A, Nouali O, Amira A. SHARE-ABE: an efficient and secure data sharing framework based on ciphertext-policy attribute-based encryption and Fog computing [J]. Cluster Computing, 2022, 25(1): 167-185.

[17] Zhang L, You W, Mu Y. Secure outsourced attribute-based sharing framework for lightweight devices in smart health systems [J]. IEEE Transactions on Services Computing, 2021, 15(5): 3019-3030.

[18] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts [C]. Proceedings of the 20th USENIX Security Symposium (USENIX Security). San Francisco, USA: IEEE, 2011: 34.

[19] El Gafif H, Toumanari A. Efficient ciphertext-policy attribute-based encryption constructions with outsourced encryption and decryption [J]. Security and Communication Networks, 2021, 2021: 1-17.

[20] Han X, Yuan Y, Wang F. Security problems on blockchain: the state of the art and future trends. Acta Automatica Sinica, 2019, 45(1): 206−225.

[21] Zeng S, Yuan Y, Ni X, et al. Scaling blockchain towards bitcoin: key technologies, constraints and related issues. Acta Automatica Sinica, 2019, 45(6): 1015−1030.

[22] Ma Z, Wang J, Gai K, et al. Fully homomorphic encryption-based privacy-preserving scheme for cross edge blockchain network [J]. Journal of Systems Architecture, 2023.

[23] Xie C, Shi R H, Zhang X, et al. Verifiable outsourcing EMRs scheme with attribute-based encryption in cloud-edge environments [J]. Journal of Information Security and Applications, 2023(Aug.): 76.