

Optimization of Digital Information Management of Financial Services Based on Artificial Intelligence in the Digital Financial Environment


Xin Li, Economics College, Jiaxing University, China

Jianxiang Zhang, Foshan University, China

Huizhen Long, Hong Kong Polytechnic University, Hong Kong

Yangfen Chen, Tianyuan College, China

Anqi Zhang, Shanghai University of International Business and Economics, China*

 <https://orcid.org/0000-0002-5878-3728>

ABSTRACT

At present, society has entered the era of digital finance, and the information management system (IMS) of financial services has been developing rapidly, so the security of data has become particularly important. Firstly, some security techniques in IMS of financial services are introduced. Secondly, this study analyzes how to combine secure multi-party computation with blockchain technology to enhance the security of IMS. Finally, the feasibility and reliability of the scheme are verified by a comparative test. The experimental results reveal that the evaluation index score of the optimized scheme is higher than that of the traditional scheme. Meanwhile, in the comparative experiment of information data encryption, it can be seen that the running time of all schemes will improve with the increase of data. However, the increase rate of the optimized model in this study is much slower than that of the traditional model.

KEYWORDS

Artificial Intelligence, Blockchain Technology, Digital Finance, Digital Information Management System, Secure Multi-Party Computation

INTRODUCTION

Digital finance is the integration of digital technology and finance, which refers to using the Internet, cloud computing, blockchain, and other digital technologies to innovate products and services provided by traditional financial institutions (Mosteanu & Faccia, 2020). Financial services' digital information management system (IMS) has been gradually optimized in this environment. However,

DOI: 10.4018/JOEUC.318478

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

with the progress of current digital emerging technologies, data privacy has become a thorny issue. Therefore, privacy computing technology comes into being (Kuznetsov et al., 2021).

Secure Multi-party Computing (SMPC), one of the privacy computing technologies, uses cryptography to protect data privacy, realize data circulation and sharing, and maximize its value, so it has received extensive attention in recent years. However, common SMPC protocols focus on developing a single practice plan for each scenario, and there are problems such as unverifiable data calculation results and an opaque calculation process, which make it difficult for the calculation party to pursue responsibility. On the other hand, blockchain technology is committed to establishing point-to-point trusted value transfer between unfamiliar nodes, and it can realize the safe sharing of data by using cryptography and consensus mechanism (Liu et al., 2020). The combination of blockchain and privacy computing not only ensures the reliability of input data but also hides the operation process (Kabir & Papadopoulos, 2019; Yan et al., 2019). However, privacy computing technology still has many problems. For example, we can infer the required password from other keys, so the protection ability is not very strong. Hence, how to solve these problems is one of the purposes and significance of the current research.

Based on this foundation, a privacy protection scheme using SMPC based on blockchain is explored to facilitate secure data sharing and collaborative computing. Firstly, related technologies of SMPC are introduced. Secondly, this study describes blockchain technology and again expounded on how to combine the two technologies to optimize the encryption scheme. Finally, a comparative test is conducted to verify the optimized scheme of this study. The innovation point is to optimize blockchain technology by integrating the two technologies and providing ideas for the optimization direction of blockchain technology (Chen et al., 2022).

LITERATURE REVIEW

For data security, Obar and Oeldorf (2020), based on the idea of crowdsourcing, implemented a privacy protection protocol for target search by using slightly homomorphic encryption and casual transport protocol. In the process of searching for the characteristic target, the protocol can protect the privacy of the target object and bystander. At the same time, the basic protocol is optimized by combining the hybrid encryption method to reduce the cost of encryption calculation. Furthermore, a deep thought-based residual learning network is trained based on the convolutional neural network to extract face feature vectors efficiently. Meanwhile, to solve the task executors' selection problem, an executor selection algorithm is proposed to find the target with maximum probability under certain budget constraints (Obar & Oeldorf, 2020). Qu et al. (2020) proposed a secure storage and sharing scheme for distributed user-sensitive data based on blockchain and International Data Encryption Algorithm (IDEA). In the model of this scheme, the data generator and the data holder are two independent subjects, which is applicable to the scenario where the data holder issues the electronic qualification certificate containing the privacy information. By improving signature algorithms, data holders can hide sensitive data from files when sharing the data and calculate a verifiable signature for the remaining data. The data visitor can verify the correctness of the extracted signature without interacting with the data generator. The characteristics of blockchain are utilized to build a decentralized access control mechanism, and the visitor attribute judgment is automatically executed through smart contracts, without the involvement of third-party trusted institutions in the entire process (Qu et al., 2020). Shen et al. (2019) designed the corresponding image storage process based on Ethereum smart contract technology for image data. They built a decentralized image storage and authentication mechanism that can be applied in practice. Based on this mechanism, they constructed the prototype system to complete the design of a smart contract for image ownership certificate authentication and transaction of use rights. This study solves the problem that traditional digital watermarking relies on a trusted third party and protects the original image by introducing Inter Planetary File System (IPFS) as a part of the whole scheme, making the whole process simpler (Shen et al., 2019).

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/optimization-of-digital-information-management-of-financial-services-based-on-artificial-intelligence-in-the-digital-financial-environment/318478

Related Content

Determinants of Social Media Impact in Local Government

Mohd Hisham Mohd Sharif, Indrit Troshaniand Robyn Davidson (2016). *Journal of Organizational and End User Computing* (pp. 82-103).

www.irma-international.org/article/determinants-of-social-media-impact-in-local-government/154004

Similarity Discriminating Algorithm for Scientific Research Projects

Chong Li, Jinjie Zhang, Anyu Wang, Xuemin Liu, Yunchsun Sun, Shibo Zhang, Zhixia Jiand Justin Z. Zhang (2023). *Journal of Organizational and End User Computing* (pp. 1-16).

www.irma-international.org/article/similarity-discriminating-algorithm-for-scientific-research-projects/332008

The Next Generation of Personalization Techniques

Gulden Uchyigit (2009). *Intelligent User Interfaces: Adaptation and Personalization Systems and Technologies* (pp. 72-92).

www.irma-international.org/chapter/next-generation-personalization-techniques/24471

Asynchronous Learning Using a Hybrid Learning Package: A Teacher Development Strategy in Geography

Kalyani Chatterjea (2008). *End-User Computing: Concepts, Methodologies, Tools, and Applications* (pp. 594-610).

www.irma-international.org/chapter/asynchronous-learning-using-hybrid-learning/18210

A Model of the Relationship among Consumer Trust, Web Design and User Attributes

Xiaoni Zhang, Victor R. Prybutok, Sherry D. Ryanand Robert Pavur (2011). *Organizational and End-User Interactions: New Explorations* (pp. 165-188).

www.irma-international.org/chapter/model-relationship-among-consumer-trust/53090