Journal of Organizational and End User Computing
Volume 35 • Issue 3

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 muti-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 Muti-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

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 Muti-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).

Nasr et al. (2019) also considered these factors. They proposed the microkernel-based virtualization multi-domain technology, which realized transparent encryption and decryption of users on mobile terminals, improving security without reducing user experience (Nasr et al., 2019). With the progress of current technology, wireless network systems have also entered people's lives. For this, Al et al. (2019) proposed a new Covert Multi-user Beam Training Strategy (CMBTS). According to the proposed CMBTS strategy, a multi-user millimeter-wave covert communication system assisted by friendly interference nodes was considered. A corresponding joint scheme of beam training and data transmission was designed to maximize the total effective covert throughput of multiple users while ensuring that the covert constraint of the Willie side of the listener was satisfied (Al et al., 2019). Based on the previous research, a new method combining SMPC-related technologies is proposed to optimize IMS (Zheng et al., 2022; Liu et al., 2021; Zhang et al., 2022).

RESEARCH METHODOLOGY

Related Technologies

SMPC's research focuses on the problem of how to safely compute a convention function when no third party is trusted. SMPC is the cryptographic basis for many applications, such as electronic elections, threshold signatures, and electronic auctions. An SMPC protocol is said to be information theory secure or unconditional secure if it is secure to an attacker with unlimited computing power. If it is secure against an attacker with polynomial computing power, it is said to be cryptographically secure or conditional secure. We consider it an essential means to solve privacy security and privacy protection problems and has produced outputs in practical application results, such as protocol and universal framework design (Knott et al., 2021). The calculation of its model is:

$$f\left(x_1, x_2 \ldots x_N\right) = \left(y_1, y_2 \ldots y_N\right) \tag{1}$$

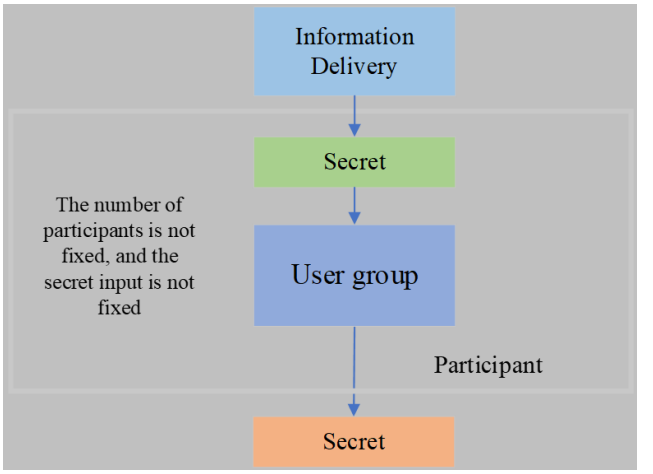
In Eq. (1), f stands for function equation; $x_1, x_2 \ldots x_N$ refers to the secret entered by the participant; $y_1, y_2 \ldots y_N$ represents the secret output to the participant after the secret passes through the model.

Secret sharing is the core of many SMPC protocols and is an essential password primitive. With the wide application of cryptosystems, key security has become a new research hotspot due to the direct connection between key and cryptosystem (Zhong et al., 2020). The idea of secret sharing is to break up secrets appropriately and securely and allocate the share of the split secrets to a group of participants to manage. Each participant only grasps one of the secret fragments, deemed a vital means to reduce key robustness and achieve key security management (Zhao et al., 2019). We can divide it into broad sense and narrow sense. The broad sense of secret sharing is a kind of idea to realize data splitting, which is widely used. In the narrow sense, it is also called arithmetic secret sharing, which randomly divides a secret number into several parts through linear operators (Volgushev et al., 2019). We display its basic principle in Figure 1.

The information is sent to the key through the computer and then translated through the ciphertext in the user's hand. Finally, the user gives feedback and saves it through the key. Different mathematical tools can be employed to construct the secret sharing scheme of threshold thresholds, which mainly consists of two phases: underground distribution and secret reconstruction (Tran et al., 2021). First, the secret distributor generates sub-secrets and sends them to the participant set. Next, the participant selects a prime from the prime set and then chooses a set of positive integers, and the following constructs the polynomial, as illustrated in Eq. (2):

$$f\left(x\right) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} p \tag{2}$$

Figure 1. Secret sharing principles



$f\left(x\right)$ expresses the constructed t-1 order polynomial; a_0 refers to the secret; $a_1....a_{t-1}$ stands for a polynomial coefficient, p represents a constant, and x is a prime. When participants want to reconstruct their secrets, the calculation reads:

$$S = f\left(0\right) = \sum_{i=1}^{k} \frac{-x_j}{x_i - x_j} p \tag{3}$$

In Eq. (3), S means the secret reconstructed by the secret restorer; $f\left(0\right)$ signifies the output result of the reconstruction function when the input is 0; x_i denotes the parameter corresponding to the secret share held by the i th participant; k expresses the number of participants, and j refers to the private share (Zhu et al., 2022). At this time, the result is the recovered secret.

As a cryptographic technique, homomorphic encryption mainly uses mathematical problems, such as ideal lattices, for construction (Wu et al., 2022). Its main feature is to design a particular encryption function to meet the requirements of different plaintext data held by various data users. In addition, the function is used to carry out operations between encrypted ciphertext data. The result obtained is equivalent to the encryption result of the corresponding plaintext data after calculation (Liu et al., 2020). Finally, an encryption function is given, which has a plaintext space and a ciphertext space. The space satisfies the following relation:

$$H\left(x\right) \circ H\left(y\right) = H\left(x \odot y\right) \tag{4}$$

$H\left(x\right)$ and $H\left(y\right)$ are the ciphertext output obtained by encrypting different inputs x & y in the plaintext space with encryption functions; $\odot$ is an arithmetic operation in the ciphertext space. If this relation is satisfied, it is proved that the encryption function has homomorphism. Two common encryption schemes are Paillier and ElGamal (Zhou et al., 2021). Paillier belongs to additive homomorphism, and ElGamal belongs to multiplicative homomorphism.

In the Paillier cryptosystem, two large prime numbers are selected, and the calculation is written as Eq. (5):

$$C = lcm\left(p-1, q-1\right) \tag{5}$$

C means the ciphertext parameter; p and q indicate prime numbers, lcm demonstrates the least common multiple of $p-1$ and $q-1$, and then any integer is selected, which needs to meet Eq. (6):

$$N = p \times q \tag{6}$$

N refers to the result of prime multiplication, and the public key finally selected is:

$$pk = \left(N, g\right) \tag{7}$$

G indicates the selected integer, pk represents the public key ciphertext, and the private key is obtained again:

$$sk = \left(p, q\right) \tag{8}$$

sk stands for the private key ciphertext. Finally, the ciphertext is obtained through the private key, as expressed in Eq. (9):

$$m = \frac{L\left(cmodN^2\right)}{L\left(gmodN^2\right)}N \tag{9}$$

m represents the ciphertext; mod implies the operation symbol, and L indicates the parameter function so that the corresponding ciphertext can be gained. The ElGamal cryptosystem is to select a large prime number, which requires a number smaller than 1 to have a significant prime number factor, then select the primitive of a module, take a random integer as the private key, as follows:

$$pk = u^d modp \tag{10}$$

d is an integer, *u* refers to primitive yuan, thus getting the public key, as revealed in Eq. (11):

$$m = C_2 \times \left(C_1\right)^{-1} modp \tag{11}$$

The password is obtained in plaintext, where C_1 and C_2 represent ciphertext.

As the underlying module of many privacy protocols, verifiable secret sharing (VSS) has developed rapidly over the past few years (Weng et al., 2019). Traditional secret-sharing schemes have sought to enhance the feasibility and efficiency of the protocol when functioning under ideal conditions. It is assumed that the secret data distributor and participant set are sincere and trustworthy and do not consider the attack situation in the mode of semi-loyal participants and malicious adversaries (Vu et al., 2020). The basic principle of the VSS scheme is that the distributor must provide additional information about the secret share and distribute it to the participants (Alexandru & Pappas, 2020). Once the participant receives their corresponding secret share, the correctness of the private share

can be verified according to the published additional information set (Bohler & Kerschbaum, 2021). In the personal reconstruction stage, each participant forwards their secret share to each other before the reconstructionist reconstructs the secret. Each node then uses the secret verification algorithm to verify the correctness of the private share provided by other participants (Stammler et al., 2022). Its schematic design is summarized in Figure 2.

Figure 2 illustrates the combination of blockchain technology and a traditional model in the scheme design. To improve on the deficiencies of the traditional model, the novel model capitalizes on the confidentiality attribute of blockchain technology. Subsequently, leveraging multiple key use boosts the security of the enhanced model.

Blockchain Technology

Blockchain is a new way of integrating applications. A distributed ledger synchronization technology combines distributed data storage, point-to-point data transmission, consensus mechanism, cryptography, and other modern information technologies. Its expression is a chain formed by many blocks linked chronologically (Ali et al., 2020). The blockchain structure is similar to a linear linked list in a data structure, and each block on the blockchain is equivalent to a node in the linked list (Lu et al., 2020). The newly created block is linked to the last block in the main chain in a head-plug manner in a linked list operation. Each block is composed of two parts, block body and head (Zhang et al., 2019). We denote its basic structure in Figure 3.

Blockchain is a distributed public ledger that can store various forms of business data, from digital asset transactions to smart contracts. According to the data stored in the practical application of blockchain technology, we divide blockchain system architecture into three eras (Taylor et al., 2020). This study describes only the infrastructure of its last generation. We can divide the blockchain infrastructure into three layers, from bottom to top, the basic network layer, the intermediate protocol layer, and the application layer. Each layer has its own specific business, and all layers interact with each other to build a decentralized trusted system (Zaghloul et al., 2020). We plot its basic structure and specific businesses in Figure 4.

The primary network layer is like the house's base, providing a compacted foundation for the upper 'building.' As a bridge, the intermediate protocol layer provides a specific service interface for the upper layer of the existing basic network environment (Mohanta et al., 2019). Finally, the application layer encapsulates examples of current problems in a variety of typical application scenarios that can

Figure 2. Schematic design of secret sharing

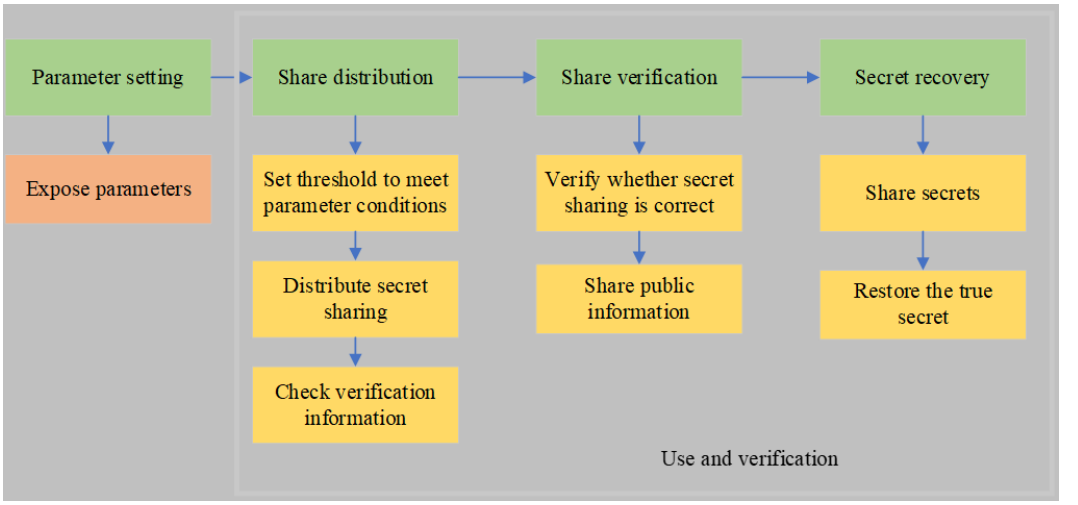


Figure 3. Basic blockchain structure

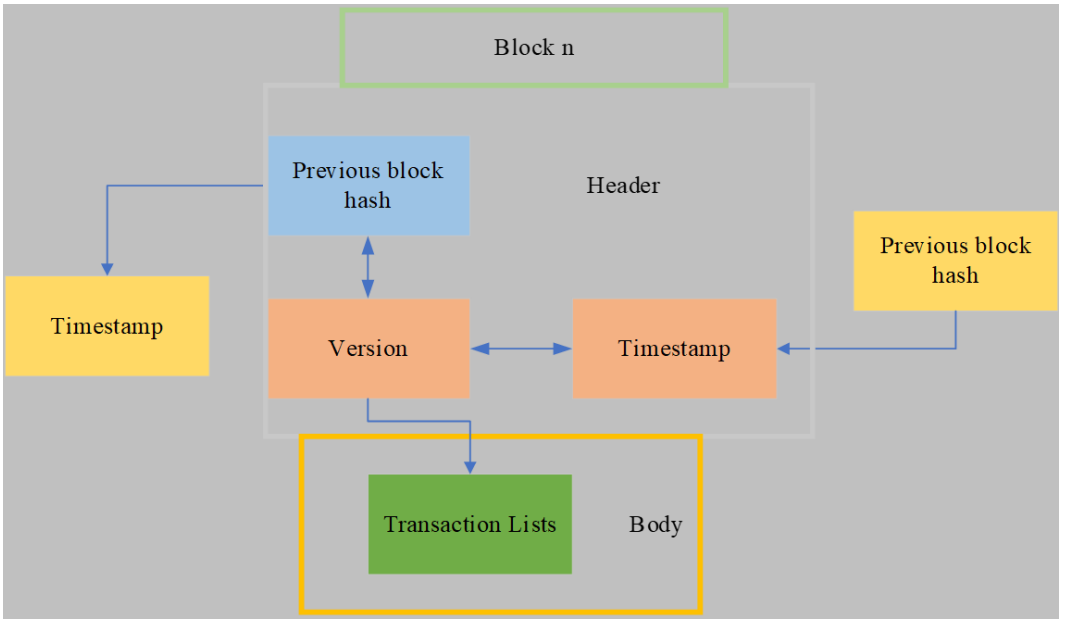
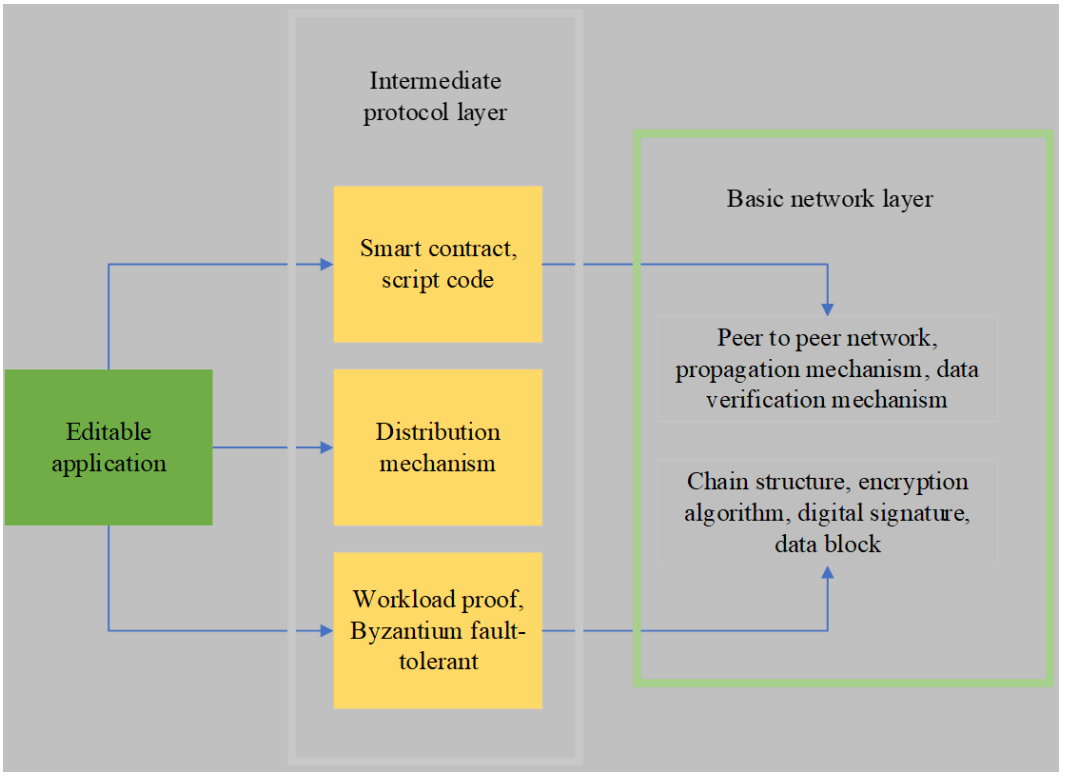


Figure 4. Blockchain infrastructure



be solved with blockchain technology. We can classify the consensus algorithm in the blockchain system into computing consensus and business consensus according to diverse dimensions of node identity. The computing consensus refers to the blockchain consensus based on computer computing power, and it provides a range of applications, primarily provides a range of applications, primarily in the fields of digital copyrighting, healthcare, public welfare, and philanthropy. Such a business consensus yields more effective results in comparison to a computing consensus, though it is contingent upon a high-credit setting. The perfect balance between efficiency and security should be considered in the application (Berdik et al., 2021; Shen et al., 2019; Feng & Chen, 2022; Chen & Du, 2022).

Privacy Protection Scheme of the Digital IMS

With the development of public key cryptography, SMPC emerges and keeps developing (Demirkan et al., 2020). SMPC deals with privacy issues in federated data computing, which has made good progress in designing specific protocols and a common framework. However, in its practical application, it is necessary to consider the additional data processing consumption caused by data privacy and security requirements, as well as the data leakage risk caused by the insecure execution environment of SMPC functions (Da et al., 2021). In designing existing blockchain-based SMPC privacy protection schemes, most use blockchain technology to provide a trusted execution environment for SMPC and use smart contracts to design incentive mechanisms to ensure the fairness of SMPC functions. Moreover, the scheme design can realize the behavior supervision of the participants. This study proposes a new protection scheme by integrating blockchain technology and SMPC.

The new scheme considers the multi-user input of the statistical computing protocol. With the characteristics of the output and the limited computing resources of the participants, as a prerequisite for data outsourcing, outsourcing computing nodes are clustered to respond to multiple outsourcing computing requests at the same time, thus making full use of the computing power of nodes in the blockchain system (Siddiqui et al., 2020). To solve the problem of data opacity in the outsourcing process of joint statistical computing tasks, blockchain is introduced to build a trusted execution environment. Nodes that perform outsourced computing tasks are incorporated into the blockchain system, and a set of intelligent contracts for node management with a punishment mechanism is constructed to strengthen the controllable management of nodes. Aiming at the problem of data privacy protection in the outsourcing process of the tasks, an outsourcing SMPC mechanism based on secret sharing is proposed to ensure that data is always presented intimately in the method of transmission and calculation. Its system model is portrayed in Figure 5.

Figure 5 denotes that compared with the traditional system; this system changes the way miners' computing power packs blocks in traditional cryptocurrency blockchain systems for profits. Compared with the traditional system, besides data, three new plates are added: distributed computing nodes, verification nodes, and SMPC participants (Mohanta et al., 2020). Blockchain provides a secure and trusted execution environment for SMPC, but data transmission and computing security is still faced with certain threats. Thereupon, a threat model is added to the verification node, as presented in Figure 6.

This scheme model considers cases where a subset of the validation nodes or a subset of the compute nodes, is maliciously controlled, and the calculate nodes are semi-honest (Honar et al., 2021). The dishonest verification node not only retains the obtained data but also forges the verification results of SMPC participants' secret input shares by reconstructing the secret input share to infer the true secret input of SMPC participants. The semi-honest compute node is very curious about the secret input and calculation results of the SMPC and may cooperate with other compute nodes to steal the input and joint calculation results of users out of interest. When the dishonest SMPC participant preprocesses the secret input data and distributes it to each computing node, it may process the secret fragment result to some extent out of interest, resulting in the deviation of the joint calculation result. The actual result can be obtained through further calculation, or multiple players may combine to analyze the input of honest participants through calculation results (Tang et al., 2022).

Figure 5. Digital information management optimization system for financial services

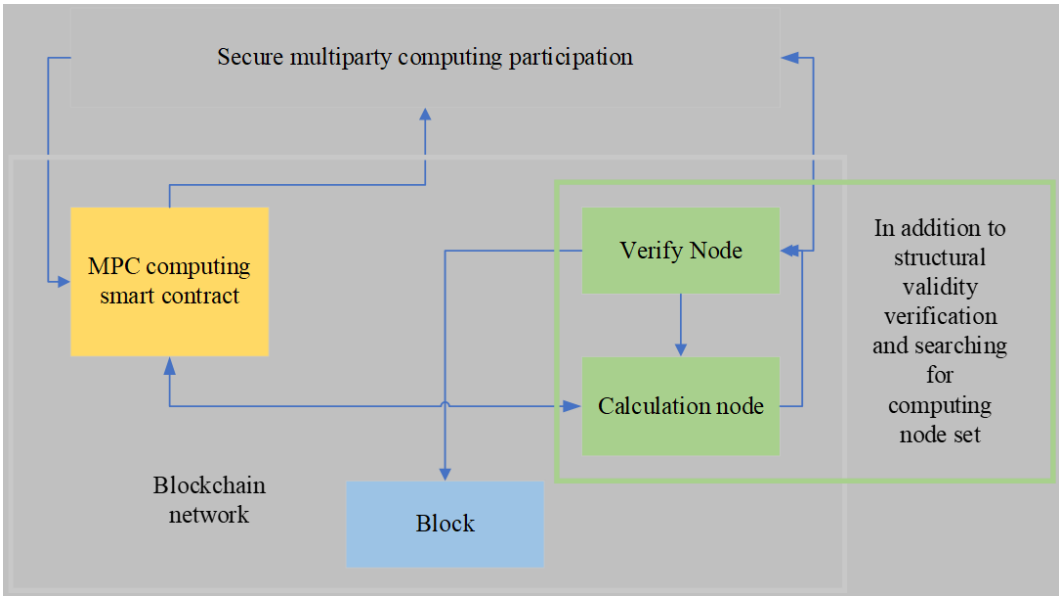
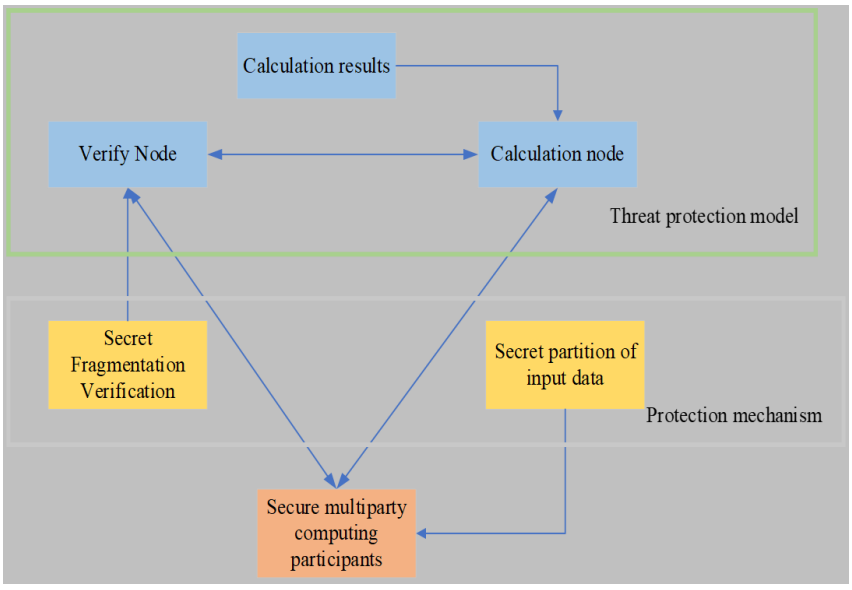


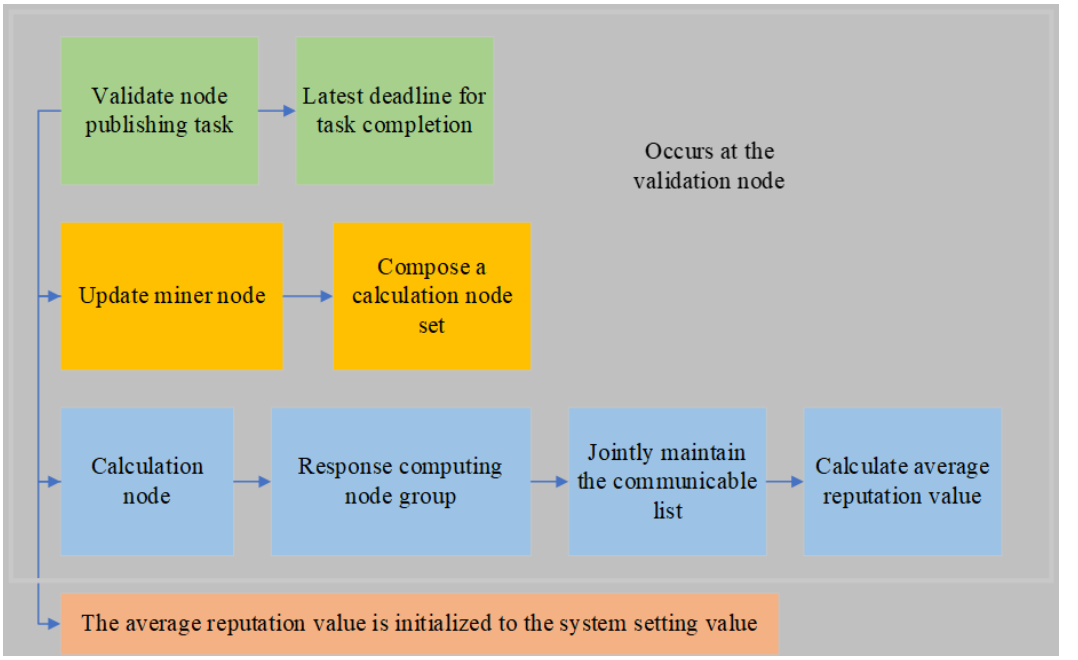
Figure 6. Threat security model



Besides increasing security, secret unlocking and refactoring need to be optimized. We can elevate decryption speed by introducing a node management mechanism to classify secrets. This process can be seen in Figure 7 and consists of an input to the contract along with the adjustment of the pertinent validation nodes.

Except for adding the node management mechanism, it is necessary to add the node incentive mechanism. It means using the distribution mechanism in the incentive layer of the blockchain system

Figure 7. Verifying the running process of nodes under the node management mechanism



to design the positive incentive mechanism so that the nodes in the system can correctly execute the protocol content and obtain the corresponding rewards. To realize the supervision and management of the data calculation process of the compute node cluster and the user node under the chain, the user node under the chain should ensure the correctness of the input secret data. While the compute node cluster must ensure the correctness of the calculation results. No additional data can be obtained during the calculation. The node incentive mechanism mainly considers two parts, and we show the specific contents in Figure 8.

As the foundation of SMPC protocol, the secret sharing scheme can effectively resist the joint attack under the threshold. In the outsourcing SMPC scheme based on private sharing, data nodes collectively input their secrets through secret sharing and then fragment them into multiple compute nodes, which perform privacy calculations according to the SMPC protocol. Meanwhile, the respective calculation results are returned to the data node through the blockchain smart contract or other trusted execution environments (Sayeed & Marco, 2019). In this way, many interactive computing processes in the process of the SMPC protocol design are "entrusted" to special computing nodes to execute, which can meet the demands of privacy and correctness at the same time. The protocol of the model also needs to be updated. The protocol has six main phases, and they exhibit their specific implementation and phases in Figure 9.

EXPERIMENTAL DESIGN AND PERFORMANCE EVALUATION

Data Set and Experimental Environment

The experiment's data set comes from a financial institution's real data, and the optimization model is tested through users' financial information. The equipment used in this experiment is the Dell EMC R740 server, in which the running memory is 64G, the total disk is 8T, the operating system is Centos7.6, and the computer language is Python.

Figure 8. Contents of the node incentive mechanism

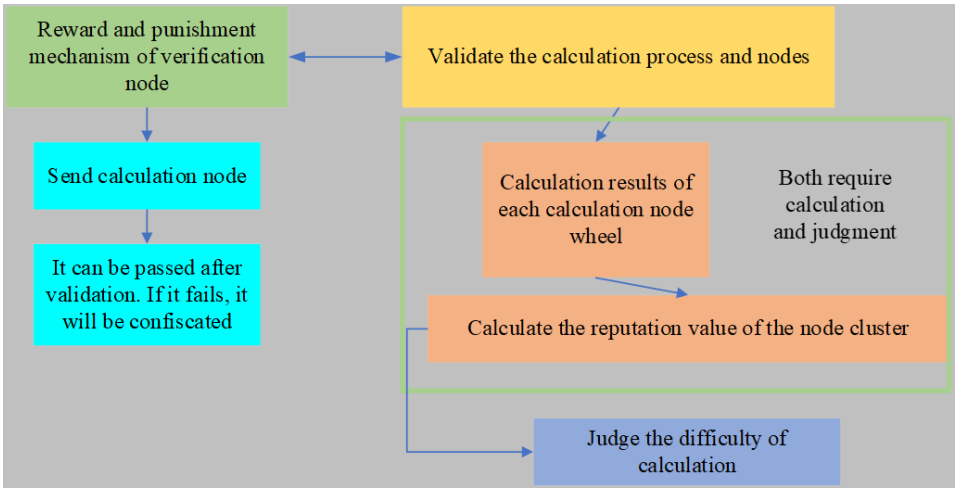
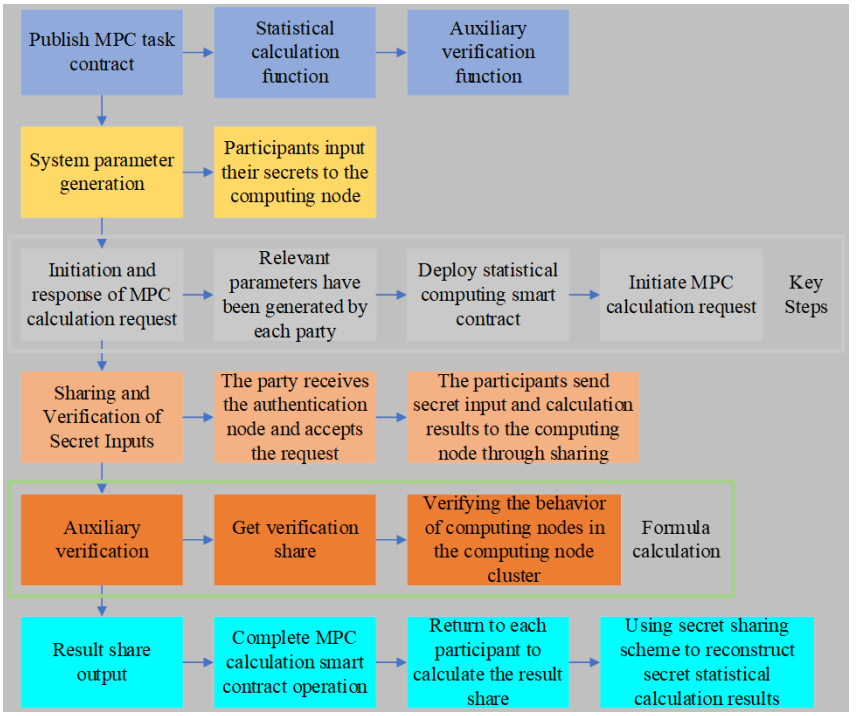


Figure 9. Post-update agreement process



Parameters

In experiment 1, fairness, scalability, robustness, privacy, and verifiability are selected for comparison. These five indicators are commonly used to evaluate security protocols. Fairness is the index data provider either can obtain the output result or cannot acquire relevant result. Scalability refers to the ease with which a protocol can be extended to more complex situations. Robustness stands for

the robustness of the protocol. Privacy means that the protocol provides privacy protection for the secret data held by the data provider. Verifiability indicates that the protocol provides authentication of the data owner's secret data. If one index is met, the score is 1; if it is not met, the score is 0. In experiment 2, the number of selected users is 50,100,150,200,250, and 300. The model's validity is verified by comparing the time consumed by information processing.

Performance Evaluation

Comparison of Evaluation Indexes Between the IMS Optimized Security Model and the Traditional Model

In the conventional model, Paillier and ElGamal encryption schemes are selected in this study, and the statistical results are demonstrated in Figure 10.

In Figure 10, the abscissa expresses the score item, and the ordinate represents the score. The total score is obtained by adding the scores of the five items. Therefore, this study's total score of the optimized information security system is 5, and the total points under Paillier and ElGamal encryption schemes are 4 and 3. Thus, the data is preprocessed in the proposed optimized encryption scheme to ensure security without affecting the results. The smart contract based on the incentive mechanism is designed to realize the controllable management of data and users. Simultaneously, the VSS scheme is employed to prevent the SMPC participants from forging the secret share, and the auxiliary private share is adopted to supervise the behavior of the computing node.

Comparison of Running Speed Between the Traditional Model and IMS Optimized Security Model

In this experiment, Paillier and ElGamal are still selected as two traditional encryption schemes for the control group, and we reveal the experimental results in Figure 11.

Figure 11 signifies that the optimized security model scheme has less running time, and with the increased number of tasks, the optimized IMS has a slower time increase rate when encrypting

Figure 10. Comparison of the evaluation indexes between the optimized security model and the traditional model

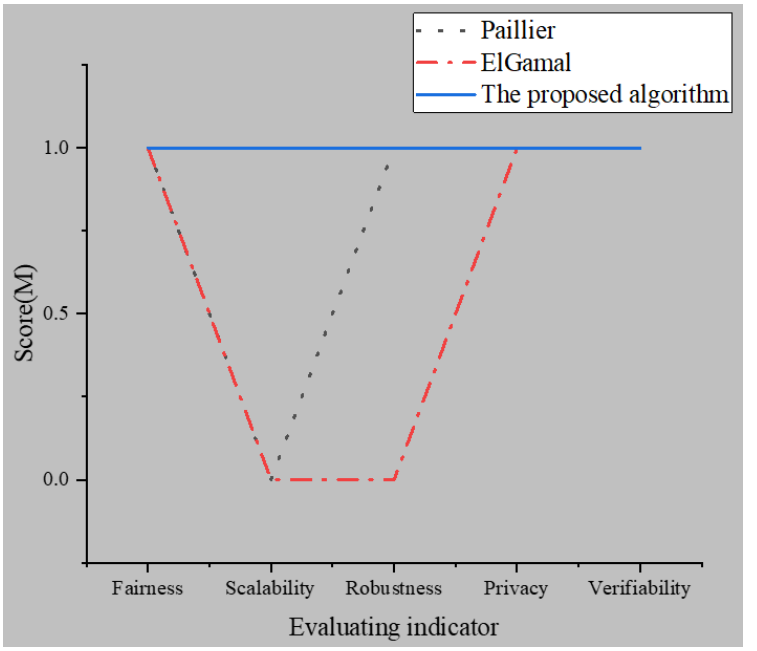
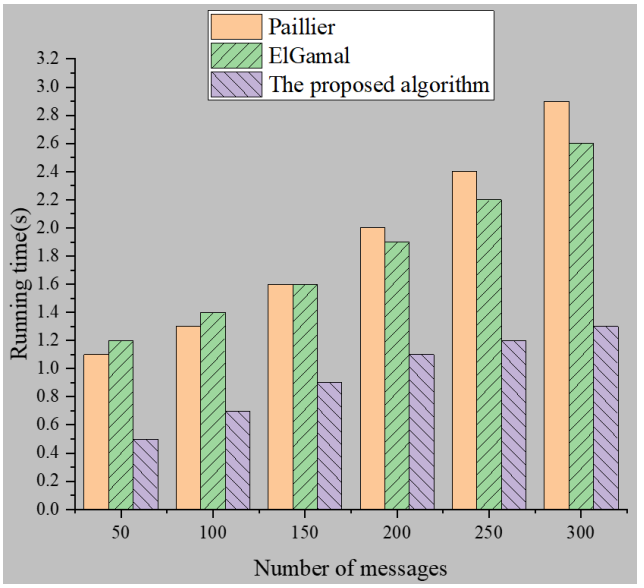


Figure 11. Comparison of operation speed between the optimized security model and the traditional model



data. When the number of tasks is 300, the gap between them is the largest. However, the rate of the running time of the ElGamal and Paillier encryption schemes is almost the same. Before the task is 150, the running time of the Paillier encryption scheme is less. After the task is 150, the running time of the ElGamal encryption scheme is slightly less than that of the Paillier encryption scheme.

Discussion

Experiment 1 details that, among the five evaluation indexes, the designed encryption scheme gets the highest score of 5, and this scheme satisfies any homomorphic statistical calculation function. Additionally, compared with the common VSS schemes, there is a small overhead in validating the validity of the verifiable secret input share. However, using a secret sharing scheme increases space consumption and computing consumption of secret input generation. It can be found from experiment 2 that the time of the three algorithm schemes will increase with the addition of the number of files. However, the increase rate of the optimized algorithm scheme here is much slower than that of the traditional algorithm scheme. Besides, with the continuous increase in the number of files, the advantages of the proposed optimized algorithm scheme will be more apparent, and the gap with the traditional algorithm encryption scheme will be larger, thus proving the rationality and effectiveness of the proposed algorithm.

CONCLUSION

With the constant development of the digital financial environment, the IMS of digital financial service of Artificial Intelligence has been optimized continuously. Therefore, with the continuous convenience of science and technology, how to protect the security of data is the top priority. Firstly, SMPC-related technologies are presented. Secondly, some applications of the current blockchain technology are described. Furthermore, the information encryption model is optimized by combining the two methods. Finally, the rationality and effectiveness of this optimized scheme are verified by comparison tests. The experimental results manifest that although the scheme in this study will increase some overhead, among the five evaluation indicators, the score is 5, which is the highest

compared with the traditional algorithm's scores of 3 and 4. Therefore, it verifies the effectiveness of the proposed scheme. Experiment 2 denotes that as the amount of information increases, the running time of traditional schemes and optimized schemes will also add. However, the proposed optimized scheme shows a significantly lower rate of time increase than the traditional model. The proposed scheme has more obvious advantages with the growing amount of information. When the number of tasks is 300, the time difference is the largest. However, there are also many shortcomings. On the one hand, the amount of information in the experiment is still too small, and we will gradually increase the data samples in future experiments. On the other hand, SMPC mainly uses random numbers and homomorphic secret-sharing methods, most of which are used when many parties are involved. Therefore, other calculation methods will be considered for optimization in the follow-up. In the future, it has been a general trend to integrate different protocols into the IMS, and the system's security can be increased by optimizing the protocols.

FUNDINGS

This work was supported by the National Social Science Foundation of China Youth Program "Research on Security Risk Early Warning Mechanism for Cross-border Flow of Enterprise Sensitive Data in the Digital Economy Era" (Grant No. 22CGL070). This research was also supported by the General Scientific Research Project of the Department of Education of Zhejiang Province: "Study on the construction and promotion of common prosperity demonstration area supported by digital agriculture" (Grant No. Y202249796). Further support was provided by the Shanghai Philosophy and Social Science Planning Youth Project "Research on Health Information Avoidance Behavior in Epidemic Prevention and Control" (Grant No. 2020EGL003) and the National Social Science Funds of China (Grant No. 21BJY251). This work was also supported by the Project name of "Exploration and research on Construction of financial comprehensive Simulation Practice Base from the perspective of school-enterprise collaborative integration" (Grant No. 22097158205119) by Industry-school Cooperative Education Project of Ministry of Education. Additional support was provided by the Student Academic Foundation of Foshan University in 2022, based on "Cultivating a Refreshing 'Soft Environment' to Build 'Hard Power' for Development: A Study on the Influencing Factors and Enhancement of Business Environment in Foshan Oriented on Entrepreneurial Satisfaction" (Grant No. xsjj202214zsa02).

REFERENCES

Al, O. A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems*, *95*(1), 511–521. doi:10.1016/j.future.2018.12.044

Alexandru, A. B., & Pappas, G. J. (2020). Secure multi-party computation for cloud-based control. In F. Farokhi (Ed.), *Privacy in dynamical systems* (pp. 179–207). Springer. doi:10.1007/978-981-15-0493-8_9

Ali, O., Ally, M., & Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. *International Journal of Information Management*, *54*(1), 102199. doi:10.1016/j.ijinfomgt.2020.102199

Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. *Information Processing & Management*, *58*(1), 102397. doi:10.1016/j.ipm.2020.102397

Böhler, J., & Kerschbaum, F. (2021). Secure multi-party computation of differentially private heavy hitters. *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2361-2377. doi:10.1145/3460120.3484557

Chen, M., & Du, W. (2022). Dynamic relationship network and international management of enterprise supply chain by particle swarm optimization algorithm under deep learning. *Expert Systems: International Journal of Knowledge Engineering and Neural Networks*. Advance online publication. doi:10.1111/exsy.13081

Chen, M., Liu, Q., Huang, S., & Dang, C. (2022). Environmental cost control system of manufacturing enterprises using artificial intelligence based on value chain of circular economy. *Enterprise Information Systems*, *16*(8-9), 1268–1287. doi:10.1080/17517575.2020.1856422

Da, L., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. *IEEE Internet of Things Journal*, *8*(13), 10452–10473. doi:10.1109/JIOT.2021.3060508

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189–208. doi:10.1080/23270012.2020.1731721

Feng, Z., & Chen, M. (2022). Platformance-based cross-border import retail e-commerce service quality evaluation using an artificial neural network analysis. *Journal of Global Information Management*, *30*(11), 1–17. Advance online publication. doi:10.4018/JGIM.306271

Honar, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Multi-layer blockchain-based security architecture for internet of things. *Sensors (Basel)*, *21*(3), 772. doi:10.3390/s21030772 PMID:33498860

Kabir, S., & Papadopoulos, Y. (2019). Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: A review. *Safety Science*, *115*(3), 154–175. doi:10.1016/j.ssci.2019.02.009

Knott, B., Venkataraman, S., Hannun, A., Sengupta, S., Ibrahim, M., & van der Maaten, L. (2021). Crypten: Secure multi-party computation meets machine learning. Advances in Neural Information Processing Systems 34 (NeurIPS 2021), 4961-4973.

Kuznetsov, N. V., Ekimova, K. V., Larina, O. I., & Lizyaeva, V. V. (2021). Financial systems development in a digital economy. In E. G. Popkova & B. S. Sergi (Eds.), *Smart Technologies' for Society, State and Economy* (pp. 1248–1255). Springer International Publishing. doi:10.1007/978-3-030-59126-7_136

Liu, J., Tian, Y., Zhou, Y., Xiao, Y., & Ansari, N. (2020). Privacy preserving distributed data mining based on secure multi-party computation. *Computer Communications*, *153*(1), 208–216. doi:10.1016/j.comcom.2020.02.014

Liu, Y., Zhang, S., Chen, M., Wu, Y., & Chen, Z. (2021). The sustainable development of financial topic detection and trend prediction by data mining. *Sustainability*, *13*(14), 7585. doi:10.3390/su13147585

Liu, Z., Zhang, A., & Wang, W. (2020). A framework for an indoor safety management system based on digital twin. *Sensors (Basel)*, *20*(20), 5771. doi:10.3390/s20205771 PMID:33053719

Lu, Y., Huang, X., Zhang, K., Maharjan, S., & Zhang, Y. (2020). Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Transactions on Vehicular Technology*, *69*(4), 4298–4311. doi:10.1109/TVT.2020.2973651

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things*, *8*(1), 100107. doi:10.1016/j.iot.2019.100107

Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2020). Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet of Things Journal*, *8*(2), 881–888. doi:10.1109/JIOT.2020.3008906

Mosteanu, N. R., & Faccia, A. (2020). Digital systems and new challenges of financial management–FinTech, XBRL, blockchain and cryptocurrencies. *Quality-Access to Success Journal*, *21*(174), 159–166.

Nasr, M., Shokri, R., & Houmansadr, A. (2019). Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. *2019 IEEE Symposium on Security and Privacy.* doi:10.1109/SP.2019.00065

Obar, J. A., & Oeldorf, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information Communication and Society*, *23*(1), 128–147. doi:10.1080/1369118X.2018.1486870

Qu, Y., Gao, L., Luan, T. H., Xiang, Y., Yu, S., Li, B., & Zheng, G. (2020). Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet of Things Journal*, *7*(6), 5171–5183. doi:10.1109/JIOT.2020.2977383

Sayeed, S., & Marco, G. H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences (Basel, Switzerland)*, *9*(9), 1788. doi:10.3390/app9091788

Shen, C.-W., Min, C., & Wang, C.-C. (2019). Analyzing the trend of O2O commerce by bilingual text mining on social media. *Computers in Human Behavior*, *101*, 474–483. doi:10.1016/j.chb.2018.09.031

Shen, M., Tang, X., Zhu, L., Du, X., & Guizani, M. (2019). Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet of Things Journal*, *6*(5), 7702–7712. doi:10.1109/JIOT.2019.2901840

Siddiqui, S. T., Ahmad, R., Shuaib, M., & Alam, S. (2020). Blockchain security threats, attacks and countermeasures. In Y.-C. Hu, S. Tiwari, M. C. Trivedi, & K. K. Mishra (Eds.), *Ambient Communications and Computer Systems* (pp. 51–62). Springer. doi:10.1007/978-981-15-1518-7_5

Stammler, S., Kussel, T., Schoppmann, P., Stampe, F., Tremper, G., Katzenbeisser, S., Hamacher, K., & Lablans, M. (2022). Mainzelliste SecureEpiLinker (MainSEL): Privacy-preserving record linkage using secure multi-party computation. *Bioinformatics (Oxford, England)*, *38*(6), 1657–1668. doi:10.1093/bioinformatics/btaa764 PMID:32871006

Tang, V., Lam, H. Y., Wu, C. H., & Ho, G. T. S. (2022). A two-echelon responsive health analytic model for triggering care plan revision in geriatric care management. *Journal of Organizational and End User Computing*, *34*(4), 1–29. Advance online publication. doi:10.4018/JOEUC.289224

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147–156. doi:10.1016/j.dcan.2019.01.005

Tran, A. T., Luong, T. D., Karnjana, J., & Huynh, V. N. (2021). An efficient approach for privacy preserving decentralized deep learning models based on secure multi-party computation. *Neurocomputing*, *422*(5), 245–262. doi:10.1016/j.neucom.2020.10.014

Volgushev, N., Schwarzkopf, M., Getchell, B., Varia, M., Lapets, A., & Bestavros, A. (2019). Conclave: Secure multi-party computation on big data. *Proceedings of the Fourteenth EuroSys Conference*. doi:10.1145/3302424.3303982

Vu, D. H., Luong, T. D., & Ho, T. B. (2020). An efficient approach for secure multi-party computation without authenticated channel. *Information Sciences*, *527*(1), 356–368. doi:10.1016/j.ins.2019.07.031

Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., & Luo, W. (2019). Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Transactions on Dependable and Secure Computing*, *18*(5), 2438–2455. doi:10.1109/TDSC.2019.2952332

Wu, Y., Wang, X., Susilo, W., Yang, G., Jiang, Z. L., Yiu, S. M., & Wang, H. (2022). Generic server-aided secure multi-party computation in cloud computing. *Computer Standards & Interfaces*, *79*(1), 103552. doi:10.1016/j.csi.2021.103552

Yan, X., Chen, M., & Chen, M.-Y. (2019). Coupling and coordination development of australian energy, economy, and ecological environment systems from 2007 to 2016. *Sustainability*, *11*(23), 6568. doi:10.3390/su11236568

Zaghloul, E., Li, T., Mutka, M. W., & Ren, J. (2020). Bitcoin and blockchain: Security and privacy. *IEEE Internet of Things Journal*, *7*(10), 10288–10313. doi:10.1109/JIOT.2020.3004273

Zhang, H., Fan, L., Chen, M., & Qiu, C. (2022). The impact of SIPOC on process reengineering and sustainability of enterprise procurement management in e-commerce environments using deep learning. *Journal of Organizational and End User Computing*, *34*(8), 1–17. Advance online publication. doi:10.4018/JOEUC.306270

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys*, *52*(3), 1–34. doi:10.1145/3316481

Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.-Z., Li, H., & Tan, Y.-A. (2019). Secure multi-party computation: Theory, practice and applications. *Information Sciences*, *476*(1), 357–372. doi:10.1016/j.ins.2018.10.024

Zheng, S., Chang, P. Y., Chen, J., Chang, Y. W., & Fan, H. C. (2022). An investigation of patient decisions to use eHealth: A view of multichannel services. *Journal of Organizational and End User Computing*, *34*(4), 1–24. doi:10.4018/JOEUC.289433

Zhong, H., Sang, Y., Zhang, Y., & Xi, Z. (2020). Secure multi-party computation on blockchain: An overview. In H. Shen & Y. Sang (Eds.), *Parallel Architectures, Algorithms and Programming* (pp. 452–460). Springer. doi:10.1007/978-981-15-2767-8_40

Zhou, J., Feng, Y., Wang, Z., & Guo, D. (2021). Using secure multi-party computation to protect privacy on a permissioned blockchain. *Sensors (Basel)*, *21*(4), 1540. doi:10.3390/s21041540 PMID:33672175

Zhu, Z., Liu, Y., Cao, X., & Dong, W. (2022). Factors affecting customer intention to adopt a mobile chronic disease management service: Differentiating age effect from experiential distance perspective. *Journal of Organizational and End User Computing*, *34*(4), 1–23. doi:10.4018/JOEUC.287910