Security analysis using blockchain based key aggregation cryptosystem with time complexity reduction

Ipseeta Nanda*[1], Lizina Khatua[2], Somashekar Reddy [3], Abhijit Ashok patil [4], Dr. Manjunath CR[5], Dr.Sathish M [6]

Abstract: One of the rapidly developing technologies that is important in the field of criminal investigation is blockchain. In recent years, security has grown to be a serious danger to every industry, including banking, supply chain management, smart applications, and the Internet of Things. In this research the proposed method has to increase the public auditing performance using blockchain based key aggregation cryptosystem (BKAC) in cloud computing. Proposed system is found to be very efficient for sharing the data then it is able to avoid and provide more security by using blockchain based key aggregate cryptosystem with the help of wallet generator. Finally, the suggested system is subjected to performance and security research to ensure that it is well suited for cloud data sharing. Time complexity must be reduced. The parameteric analysis has been carried out in terms of Completion Ratio, Throughput, Degree of Imbalance, Scalability, QoS. . the proposed technique attained Completion Ratio of 61%, Throughput of 92%, Degree of Imbalance of 66%, Scalability of 67%, QoS of 62%.

Keywords: *Blockchain, cloud computing, key aggregation, security, time complexity*

1. Introduction

Blockchain technology will be the solution in next generation of information technology [1]. As a result of its distinct technological advantages, cutting-edge value theories, and numerous application scenarios, blockchain technology is currently developing into a frontier field of high value. Many experts even predict that blockchain technology, which follows the steam engine, power, information, and Internet technologies, will be the one to spark the next disruptive revolution [2]. The physical infrastructure is often owned and maintained by a hosting provider, and the digital data is stored in logical pools across numerous servers (and frequently regions) in cloud storage. These cloud storage companies are in charge of maintaining the physical environment's security and functionality as well as the data's availability and accessibility [3]. In terms of accessible interfaces, almost instantaneous elasticity and scalability, multitenancy, and metered resources, cloud storage is similar to larger cloud computing because it is built on infrastructure that is heavily virtualized. Cloud storage solutions can be installed on-site or used through an off-site service. Although the phrase "cloud storage" was originally used to describe a hosted object storage service, it has come to refer to various types of data storage that are now offered as a service, such as block storage. A crucial application of cloud computing is dada sharing. Within the cloud, data can be downloaded or uploaded. Any kind of data can be kept on the cloud. As a result, the data that is shared may be in text format or in a multimedia format. This data exchange should be done in a flexible, effective, and safe manner. Otherwise, a hacker might get our personal information and utilise it inappropriately. Distributed networks, blockchain, and cloud computing have unique qualities and face comparable network-related difficulties. A higher degree of coverage that integrates various network-related technologies could include future integration. Although adversary techniques may differ, a few cyber threats in cloud computing, for example, identity theft and data mining-based attacks, also apply to blockchain networks [4].

The contribution of this research is as follows:

1. the proposed method has to increase the public auditing performance using blockchain based key aggregation cryptosystem (BKAC) in cloud computing.

Faculty of Information Technology, Gopal Narayan Singh University,Jamuhar,Rohtas Bihar,India
ipseeta.nanda@gmail.com
[2]*School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar, India, ipseeta.nanda@gmail.com*
[3]*Assistant Professor, Department of Computer Science and Engineering Jain(Deemed-to-be University), Bangalore, India*
EmailId : r.somashekar@jainuniversity.ac.in
[4]*Assistant Professor, Bharati Vidyapeeth (Deemed to be University) Y. M. Institute of Management Karad, Abhijit.patil@bharatividyapeeth.edu*
[5]*Associate Professor, Department of Computer Science Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, cr.manjunath@jainuniversity.ac.in*
[6] *Associate Professor, Electronics and Communication Engineering, Rajalakshmi Engineering College,sathish.m@rajalakshmi.edu.in*

2. Proposed system is found to be very efficient for sharing data then it is able to avoid and provide more security by using blockchain based key aggregate cryptosystem with the help of wallet generator.

2. Related works

Surveys on trust protocols in cloud computing systems have already been conducted. Work [5] investigated consumer trust issues with cloud computing platforms to assist service providers in changing their behaviour. Work [6] reviewed the benefits and drawbacks of relevant studies in order to assess trust approaches in cloud computing. A thorough introduction to the existing trust models in cloud systems was provided by author [7]. Work [8] conducted an assessment of the available trust mechanisms and outlined their shortcomings. An outline of trust management in cloud services was provided by author [9] along with a discussion of the unresolved challenges. Work [10] provided a survey of cloud computing trust solutions to evaluate service providers' performance. After discussing potential assaults on cloud systems, author [11] gave an outline of the current trust-based strategies. In order to characterise trust in a cloud environment, research [12] constructed a conceptual model and surveyed 43 similar techniques. The most recent trust evaluation techniques used in cloud computing systems were examined in work [13]. A taxonomy and classification of trust models and trust evaluation techniques in the cloud paradigm were offered by the author [14]. A survey on the taxonomy of trust elements and evaluation techniques was conducted by work [15] to assist cloud users in making reliable service provider selections. Researchers have paid close attention to the blockchain technology since its inception, particularly given how well-liked it is in e-currencies. We can currently locate a lot of blockchain reviews.

3. Proposed blockchain based key aggregation cryptosystem

This section discuss novel technique in public auditing performance using blockchain based key aggregation cryptosystem (BKAC) in cloud computing. Proposed system is found to be very efficient for sharing data then it is able to avoid and provide more security by using blockchain based key aggregate cryptosystem with the help of wallet generator.

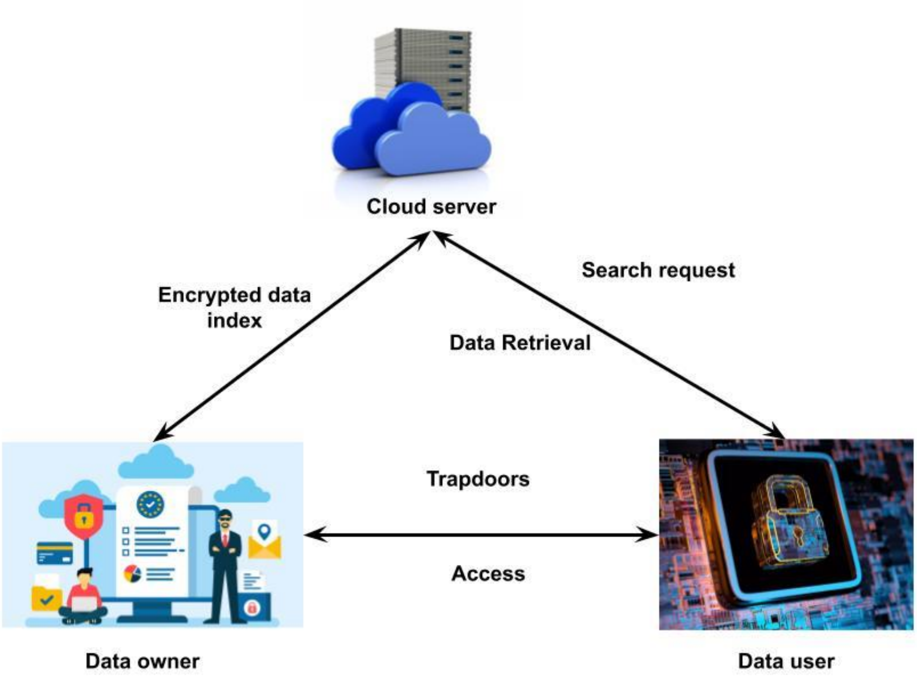

Figure-1 Blockchain based Cloud Data Framework

$$\left((y_1, a_1, \sigma_1), \cdots, (y_n, a_n, \sigma_n), (v_1, \pi_1), \cdots, (v_m, \pi_m), t\right)$$
(1)

The inputs of Txx are triples (y1, a1, 1), yn, an, n), where yi is the hash of a prior transaction. Txyi is also known as an input script, and ai is an index of Txyi's output. Similar processes can be implemented in Ethereum based on the Ethereum Alarm Clock. Furthermore, eq is used to represent the body of Txx. (2)

$$[\mathrm{Tx}_x] = \left((y_1, a_1), \cdots, (y_n, a_n), (v_1, \pi_1), \cdots, (v_m, \pi_m), t\right)$$
(2)

$$e(\sigma, g) = e\left(\prod_{i=1}^{i_i} \sigma_i^e, g\right) = e\left(\prod_{i=1}^{r} \left(h(f_i) \cdot u^{f_i}\right)^{k\dot{\alpha}}, g\right)$$

$$= e\left(\prod_{i=1}^{r} \left(h(f_i) \cdot u^{f_i}\right)^{al}, g\right) = e\left(\prod_{i=1}^{r_i} h(f_i)^0 \cdot \prod_{i=1}^{i} u^{f,9}, g\right)$$
(3)

$$= e\left(\prod_{i=1}^{r} h(f_i)^a \cdot u^{\Sigma_{i=1}^{m}}, v\right)$$

$$e\left(\prod_{i=1}^{r} h(f_i)^m \cdot u^{\mu}, v\right) = e\left(\prod_{i=1}^{r} h(f_i)^{u_h} \cdot u^{\Sigma_{i=1}^{i_i \cdot a}}, v\right)$$

The equations' equality on both sides is evident. Therefore, eq determines whether the data's integrity is intact by determining the equation's equilibrium (4).

$$\text{proof} = \left\{\mu, \sigma, \left(h(f_i)\right)_{1 \le i \le s_e}\right\} \quad (4)$$

Question that we have is whether the public key, which we will name Q, is equal to the private key times G by eq. On this curve, we have an X and a broad but a private key is just a scalar about you (5).

$Q = P \cdot g$ (5)

If you try to find the value of P in the oval where Q and G have values using a huge private prime Y large integer, you will find that it is rather challenging. Equation (6) for elliptic curve cryptography is as

$y^2 = x^3 + ax + b$ (6)

$PK_A = R_A \times G$ and $PK_A = P_A \times G$ (7)

$S = R \times RP_A$ (8)

This is the same secret key that the receiver also created, which is made up of 100 Internet of Things (IOT) devices (9).

$S = r \times P_A$ (9)

$$e\left(V, pk_1 \cdot R_1 \cdot g^{H_1(ID,U_0,X_0)} P_{pub} \cdot g^{h_1}\right)$$
$$= e\left(V, g^{\vec{u}} \cdot g^{\vec{r}_1} \cdot g^{H_1(ID,U_0,X_0)} g^{\vec{s}} \cdot g^{h_1}\right)$$
$$= e\left(g^{(d_{ID}+h)^{-1}}, g^{\vec{u}+\vec{r}_1+H_1(ID,U_0,X_0)+\vec{s}+h_1}\right)$$
$$= e(g,g)^{(\vec{u}+u_0+H_1+\vec{s}+h)^{-1}} \cdot e(g,g)^{(\vec{u}+u_1+H_1+\vec{s}+h_1)} = e(g,g)$$

(10)

$$\left(\frac{K_a}{e(\Pi_{jes} g_j, v^T)}\right)^{-r} = \left(\frac{I^T \cdot e(K_S^r, g)}{e(\Pi_{j\in S} g_j, v^T)}\right)^{-T} = I \quad (11)$$

The cloud server can determine identify of user seeking to download files from the aforementioned equation. It is common knowledge that gi where I = 1,...,3n is public. Additionally, the application requesting the download of files provides the secret key Ka, the secret key's expiration date, T, and indices, S, of ciphertext classes. Cloud server can quickly calculate this equation with all of these components. The server can decide whether to approve the requested download by comparing I with I ′. Furthermore, if the result of this calculation equals I, S and T are unquestionable. In light of fact that index is contained in S and time T is, the delegatee is able to download ciphertext classes.

$$c_3 \cdot= c_1 \cdot \frac{e(\Pi_{iss} g_{zi+j} \cdot g^x)}{e\left(\Pi_{jes} g_j \cdot g_{21})^x\right) \cdot e(g_{3i} \cdot g^2)}$$
$$\frac{e\left(K_1 \cdot \Pi_{jesj+i} g_{g_{il}+j,c_1}\right)}{e\left(\Pi_{jes} g_j, c_2\right)}$$
$$\cdot\, c_3 \cdot \frac{e(\Pi_{jes} g_j^r \cdot \Pi_{jesjest} g_{2i+1}, g^z)}{e(\Pi_{j\in S} g_j, (v \cdot g_{21})^x)} \quad (14)$$

This derivation demonstrates that the delegatee can successfully decrypt ciphertexts using Ks and param. Furthermore, n, total number of ciphertext classes, has no effect on the ciphertexts created by Encrypt, aggregate keys created by Extract, or any of other components of Decrypt. This means that regardless of how frequently n is modified, the KAAC method is appropriate for dynamic cloud storage. 3) For safety: As we can see:

4. Experimental analysis

In our implementation, cryptographic operations are implemented using the M iracl library, a source library concerning pairing computing. We're going to pick Type-1 pairing. The curve Y 2=X3 + X over field Fp is formed, and it is quickest (symmetric) pairing of all types of curves, for some prime p = 3 mod 4. It has a 2GB RAM. (2) Computer: We performed the test using Ubuntu 18.04.1 LT S in a virtual computer. The operating system is Windows 7 Ultimate, 64-bit 6.1.7601, Service Pack 1. The physical computer is written in C++ and has an Intel(R) Core(TM) i7-3630QM CPU running at 2.40GHz plus 4. (3) assembling and connecting our programme: Android Debug Bridge Kit is the connecting tool. Additionally, for personal computers and mobile phones, gcc version 4.8.4 and the arm-none-linux-gnueabi cross-compiler are used.

Table-1 Comparison of proposed and existing techniques

Parameters	**MAS**	**CNN**	**SA_BKAC_TCR**
Completion ratio	55	58	61
Throughput	85	88	92
Degree of Imbalance	59	61	66
Scalability	63	65	67
QoS	53	55	62

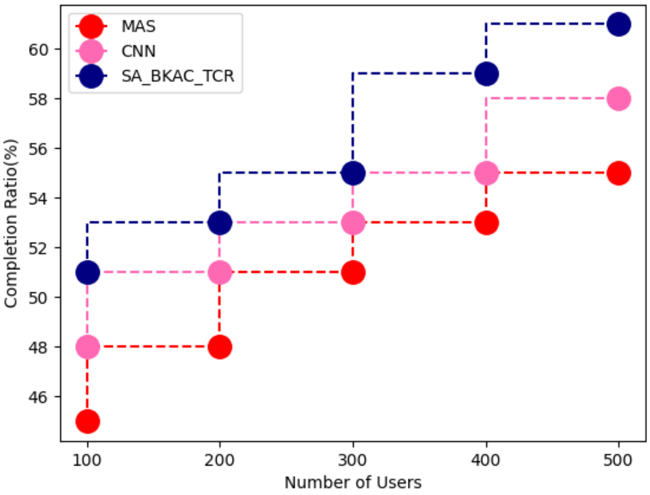

Figure-2 Comparison of Completion Ratio

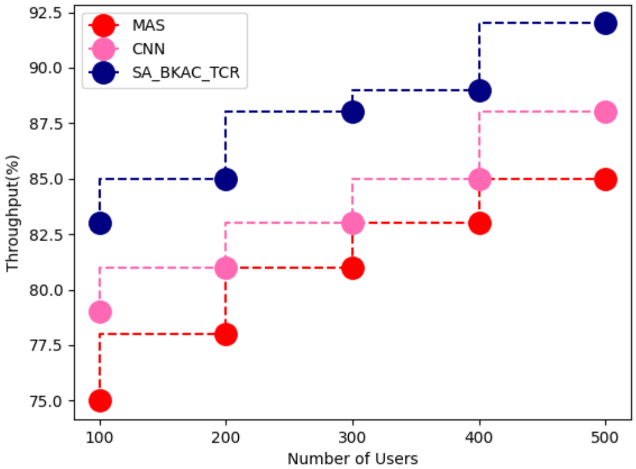

Figure-3 Comparison of Throughput

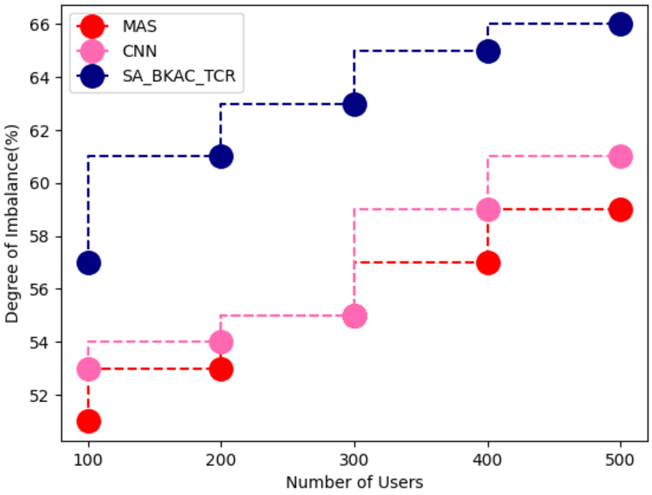

Figure-4 Comparison of Degree of Imbalance

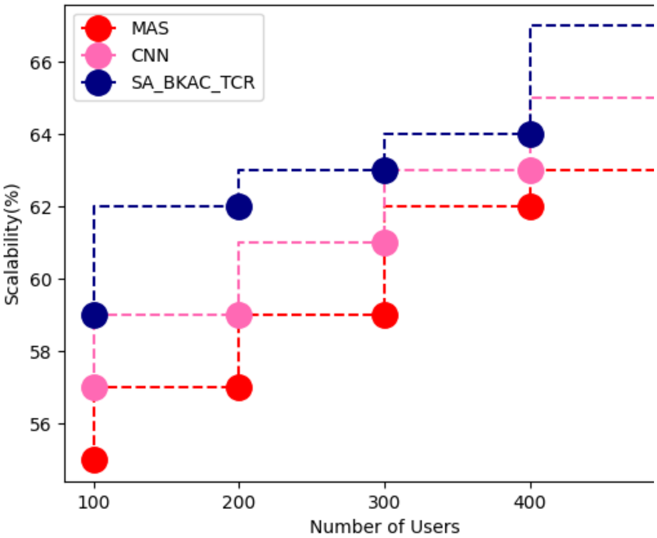

Figure-5 Comparison of Scalability

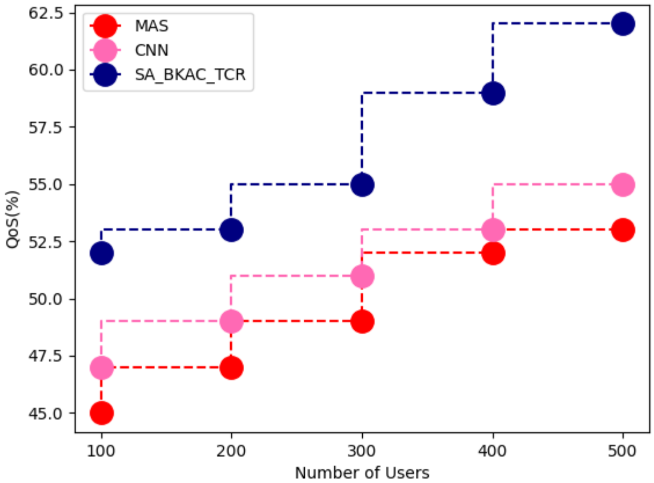

Figure-6 Comparison of QoS

A large number of delegation decryption keys could raise communication costs and the chance of data leaking. Because of its connection to the expense of storage, we also pay special attention to the ciphertext's size. The production of the decryption keys in various key assignment methods is dependent on prior file classifications. The structure of the file classifications must change when a new class of files is uploaded to cloud server. Users can also alter the classification process. Key-aggregate encryption simply cannot change to fit this circumstance. Our encryption method, KAAC, may provide ciphertext and decryption keys of a fixed size. Additionally, it has no bearing on file classification because our system allows for regular file update. The height of the tree that we defined was denoted by letters h, where h had the values 8, 12, and 16. These three structures have a total of 256, 4096, and 65,536 nodes, respectively. We discovered that when r = 0.7, the ratio of na to N rose to 38%. Additionally, we discovered that the ratio of na to N rose from r = 0.1 to 0.7. When the ratio of na N was substantially lower than 0.38 and the r value was less than 0.5. In addition, we may estimate the number of keys needed for the tree-based key assignment scheme using this table. Proposed method's completion ratio was 61%, throughput was 92%, the degree of imbalance was 66%, scalability was 67%, and QoS was 62% based on the analysis above.

5. Conclusion

Task scheduling is a process of mapping the corresponding task to its allocated resources. But in reality, the problem of mapping tasks to a massive amount of resources is categorized under NP-hard problems. The algorithms which can provide an optimal solution in less time for the NP-hard problems in cloud computing hardly exist. Since to solve problem of resource allocation and task scheduling that exist as major criteria in cloud computing, this research is initiated. This research propose novel technique in security by using blockchain based key aggregate cryptosystem with the help of wallet generator. the proposed method has to increase the public auditing performance using blockchain based key aggregation cryptosystem (BKAC) in cloud computing. the proposed technique attained Completion Ratio of 61%, Throughput of 92%, Degree of Imbalance of 66%, Scalability of 67%, QoS of 62%. We intend to address this issue in future work by storing only the latest blocks. In fact, the user does not need to keep all of the blockchain in storage for a very long time. To maintain the immutability of the blockchain, it can only save hash of preceding blocks, not actual blocks.

References

[1] Singh, P., Masud, M., Hossain, M. S., & Kaur, A. (2021). Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid. *Computers & Electrical Engineering*, *93*, 107209.

[2] Hong, Z., Zhou, L., Zhan, Y., Liu, C., & Wang, B. (2022). Cryptanalysis of an additively homomorphic public key encryption scheme. *Computer Standards & Interfaces*, *82*, 103623.

[3] Jia, B., Zhang, X., Liu, J., Zhang, Y., Huang, K., & Liang, Y. (2021). Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. *IEEE Transactions on Industrial Informatics*, *18*(6), 4049-4058.

[4] Yang, Y., He, D., Vijayakumar, P., Gupta, B. B., & Xie, Q. (2022). An Efficient Identity-based Aggregate Signcryption Scheme with Blockchain for IoT-enabled Maritime Transportation System. *IEEE Transactions on Green Communications and Networking*.

[5] Saha, R., Kumar, G., Devgun, T., Buchanan, W., Thomas, R., Alazab, M., ... & Rodrigues, J. (2021). A Blockchain Framework in Post-Quantum Decentralization. *IEEE Transactions on Services Computing*.

[6] Wang, T., Wang, J., Yang, Q., Yang, B., Li, H., Xu, F., & Qiao, Z. (2022). An Efficient Verifiable Searchable Encryption Scheme with Aggregating Authorization for Blockchain-Enabled IoT. *IEEE Internet of Things Journal*.

[7] Loukil, F., Ghedira-Guegan, C., Boukadi, K., & Benharkat, A. N. (2021). Privacy-preserving IoT data aggregation based on blockchain and homomorphic encryption. *Sensors*, *21*(7), 2452.

[8] Li, H., Wang, T., Qiao, Z., Yang, B., Gong, Y., Wang, J., &

Qiu, G. (2021). Blockchain-based searchable encryption with efficient result verification and fair payment. *Journal of Information Security and Applications*, *58*, 102791.

[9] Regueiro, C., Seco, I., de Diego, S., Lage, O., & Etxebarria, L. (2021). Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption. *Information Processing & Management*, *58*(6), 102745.

[10] Liu, D., Wu, H., Huang, C., Ni, J., & Shen, X. (2022). Blockchain-based Credential Management for Anonymous Authentication in SAGVN. *IEEE Journal on Selected Areas in Communications*.

[11] Li, J., & Zhang, K. (2022, January). Intelligent transportation big data retrieval algorithm based on blockchain and aggregation signature. In *2022 IEEE 2nd International Conference on Power, Electronics and Computer Applications (ICPECA)* (pp. 704-711). IEEE.

[12] Subathra, G., Antonidoss, A., & Singh, B. K. (2022). Decentralized Consensus Blockchain and IPFS-Based Data Aggregation for Efficient Data Storage Scheme. *Security and Communication Networks*, *2022*.

[13] Singh, C., & Jagatheeswari, A. (2022). Secured blind digital certificate and Lamport Merkle cloud assisted medical image sharing using blockchain. *Multimedia Tools and Applications*, 1-20.

[14] Tian, H., Jian, Y., & Ge, X. (2022). Blockchain-based AMI framework for data security and privacy protection. *Sustainable Energy, Grids and Networks*, *32*, 100807.

[15] Zhang, L., Zou, Y., Yousuf, M. H., Wang, W., Jin, Z., Su, Y., & Kim, S. (2022). BDSS: Blockchain-based Data Sharing Scheme With Fine-grained Access Control And Permission Revocation In Medical Environment. *KSII Transactions on Internet and Information Systems (TIIS)*, *16*(5), 1634-1652.

.