IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMPLEMENTATION OF A PROXY REENCRYPTION METHOD FOR SECURE DATA SHARING USING BLOCKCHAIN

[1] JAYA J. KURIL, [2] PROF. H. R. VYAWAHARE

[1] P.G Student, Department of Computer Science & Engineering, Sipna C.O.E.T, Amravati, India,
[2] Assistant Professor, Department of Computer Science & Engineering, Sipna C.O.E.T, Amravati, India.

Abstract: Data sharing is important IoT application in cloud computing. Unauthorized data use is a major issue with this technology, and the consequences can be disastrous. This article discusses a method for securing data sharing in the cloud. Identity-based encryption can be used by cloud service providers to protect data in the cloud. Because of its limited resources, an Internet of Things Edge device (node) behaves like a proxy server to get the most complex statistics computation. As a result of implementing information-centric networking features, our service quality and bandwidth utilization have both improved. The blockchain enables decentralized data sharing in our system model. Fine-grained access control reduces central system bottlenecks. With our approach, we have seen promising results in a data security evaluation and analysis

Index Terms **- Blockchain Technology, Cloud Computing Technology,Internet of Things IoT, Information Technology, Proxy Server, Data Sharing, Security**

I. INTRODUCTION

The rapid development of information diversification, cloud storage is becoming progressively popular in our daily life. Cloud storage allows businesses or individuals to access cloud data anytime, anywhere, and this feature provides incredible access to our lives.

First, shared data must be encrypted to ensure data confidentiality. Second, the complexity of data security is increasing and the efficiency of data exchange is decreasing. Many cloud storage systems are also managed by a centralized company with powerful storage and monitoring, so the company must consider a third party to inherit any failure. am. Finally, it is important to update the cloud storage of the equipment, and with an increase in employee wages, the centralized cloud storage cost is rapidly increasing. Therefore, you must implement flexible access control through encrypted data to better ensure the confidentiality of data and data availability, and you must move data storage devices from a centralized system to a distributed system, not inexpensive than an existing centralized storage system.

Yu, Y. et al (2018) The Internet of Things provides tremendous convenience to people's daily lives by exchanging data and making full judgments. However, it creates security and privacy concerns. Blockchain technology has the abilty to overcome these privacy concerns in the IoT. In this article, they talk over the most prevalent privacy issues with the IoT. Then, in order to address these issues, blockchain-based solutions are given [6].

H. Xu et. al. (2020) A BSDS-FA os a block chain based technology is being developed to address the issue of privacy leaks at the time of data sharing in the internet with the help of fine access control mechanism. To begin, this article introduces a novel hierarchical attribute-based encryption technique that makes use of both a hierarchical and a multi-level authorization structure. By allocating separate user characteristics to distinct authorization centres, the approach enables fine-grained access control(FA). On a blockchain, a smart contract performs partial decryption to minimize user decryption costs. Additionally, blockchain technology enables the tracability of earlier acts, which satisfies data security standards for restriction, openness, and transparency. [11]

J. Lu, J. Shen et. al. (2021) By merging IoT technologies in industrial settings, the Industrial Internet of Things.IIoT enables the construction of smart factories. It gathers data from industrial devices by employing a number of sensors. Cloud storage enables data storage to be outsourced, which is especially useful for sensors with limited on-board storage and processing capability. To ensure that devices keep their privacy, gathered data should be kept in ciphertext format. As a result, data analysis from devices should be done through encrypted data sharing. This article discusses a sensor sensor storage system that is cloud-based. An new group signature mechanism is employed initially to provide anonymous authentication to assure the security and efficiency of data sharing and storage. [13].

II. PROBLEM DEFINITION:

In IoT data sharing has spread in recent years to systems from medical and smart homes to automotive networks and electricity transactions. When an IoT device (such as a sensor, Smartphone, or Smartwatch) transmits data to another person, the data is typically encrypted and sent to a cloud storage service. Access control rights and data binding rights are used to protect privacy, make systems easier to use, and prevent bad behavior on the network. Figure 3 depicts a typical conversational style.
In this type of system, the data producer is the main business that produces the data. You can encrypt data and participate in data protection for illegal users that export to CLOUD Service Provider (CSP). Therefore, data processing is not necessarily a difference between data producers and data owners because data processing must not be translated. The data owner is the central part of the data holder. The data owner generates an arbitrary number to encrypt the data before downloading and sharing the user. Data access is performed and the data owner can be a manufacturer. However, this does not mean that a variety of organizations can participate in data production. a trusted server computer/server system.

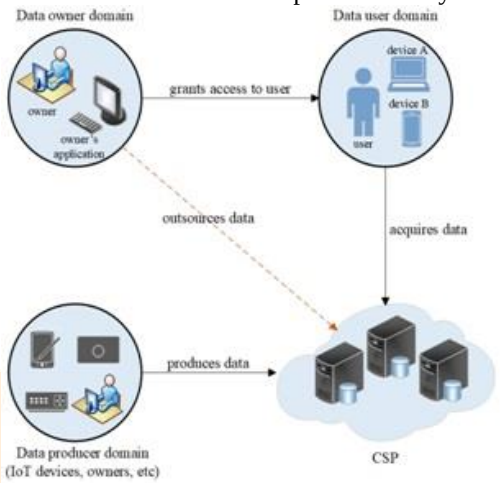

Fig.3 Simple Data Sharing Platform

User data domains contain the official recipients of information shared by owners. Users include people as well as devices. These data users must have access to shared data on the CSP, a less trusted group that provides data storage services. Stores encrypted data for owners and accesses data through secure communication channels. Provides data exchange services, but cannot read content in plain text. This means that all access information must be encrypted and only accessible to those who require it. However, because the data is so trustworthy, CSPs may wish to try to read it. Before starting to share data, user 2 may want to look at data that has already been shared between the delegator and data user. Edge nodes send delegate their ID or credentials instead of getting the same data from a cloud server to provide better service and use less bandwidth. There's also encryption and other issues to consider. This saves money and speeds up the network.

III. SYSTEM ARCHITECTURE:

The rapid development of cloud storage has greatly contributed to industrial productivity and social development. However, with the advent of the big data era, cloud storage faces many challenges, including the complexity of managing data security, the efficiency of data exchange, and the cost of points of failure. The Proxy Re-encryption (PRE) encryption primitive is considered a good technique to improve data efficiency and security. Blockchain can overcome loopholes caused by point failure. Both of these methods have received a lot of attention in recent years. However, the existing PRE method requires complex certificate management and blockchain is not suitable for big data storage due to its high cost. To solve the above problems, this article proposes IBPRE, Data OwnerManipulation IBPRE (DMIBPRE), a new IBPRE (Identity-Based Proxy Re-Encryption) method that can be implemented using blockchain and obtained in combination.

To make data available to a wide range of recipients, many systems now use cloud-based solutions. Storage, access management, and business intelligence are all provided by third-party cloud service providers [5]. In this scenario, both data makers and data users may need the services of third-party service providers. In addition, the sender and customer must agree on the amount of data to be sent and the cost of doing so. [6] These agreements do not require the consent of the IoT. In general, establishing these agreements requires considerable time and effort. As a result data transmission is delayed.

In addition, it is necessary to assess the accuracy of the data. As a result, any third-party source is not entirely reliable. Data collected from IoT devices and other external sources are not altered in any way. Meeting the requirements of future IoT systems will be difficult if the current IoT core architecture is not relied upon.

For this purpose, we propose to focus on the issue of data sharing with hybrid cloud storage architecture. We will also talk about how to use the strategy. We have developed a very effective proxy re-encryption system to protect the data of the Smart Contract Holder and other people present during operation. In this guide we will learn about storing data from cloud servers and connecting to blockchain. The hybrid architecture prototype and proxy rewriting scheme are tested at its speed in the test bed to ensure its effectiveness. Cloud-based commercial service providers and computer components were used to create the prototype. The scale and performance of the method are demonstrated by looking at several different performance metrics. That way, we can see what our solution might be to explore the real world situation. To understand how these blockchain platforms work, it is important to look at their shortcomings.

Representative re-enactment was first proposed by Blaze et al. [2] Allows the holder to convert the file created under the owner's public key into encryption at the data recipient. Suppose a data owner is represented and a data user is represented. Under this program, the messenger can temporarily send encrypted messages to the messenger without disclosing his or her private key. A messenger key you create for yourself or a trusted third party key, such as a reset key. A key proxy uses an encryption algorithm that recovers cipher text before sending new deleted encryption to the user. A basic feature of the proxy encryption system is that

the proxy is not fully trusted which means the private key holder of the data is unknown to them. It is considered to be the primary user access to encrypted data, which is an essential element in any data sharing method. In addition, the proxy encryption system allows encrypted data to be shared between authorized users, while maintaining its privacy on illegal groups. Encryption usage reduces data exposure so users sent only by the data owner can access the exported data.

With the help of this example, this article proposes a way to improve data sharing on IoT by integrating proprietary-based encryption, an information-based network and proxy re-encryption with blockchain technology. Shamir [3] first introduced the concept of identity-based encryption, in which the sender encrypt the message using an email identifier as a public key. It is a very powerful method used to combat many major distribution problems and has been used on many cryptographic protocols such as searchable public key encryption [4], [5], encrypted shaking [6]] and selected ciphertext attacks. Included in the development. Protect encryption keys for public keys [7]. Identifier-based encryption encryption is preferred because it involves a large amount of data encryption, encryption, and key management, and these methods are not compatible with IoT device-restricted devices. We have introduced the idea of sharing data from a data network, where data owners can distribute different names to their data and replicate them in network repositories [12], [13]. This ensures that the IoT ecosystem requires efficient data distribution and network and wide bandwidth. Nakamoto [14] introduced a nationally distributed, distributed system that helps secure and reliable data sharing on trust issues. It has attracted a lot of attention because of its blockchain technology and ability to manage data privacy. Despite development problems when large amounts of data are stored, emerging system applications have used the blockchain to control access to data management. Data privacy and user withdrawals can also be accessed using the blockchain.

Enables security and privacy in data sharing systems through proxy reencryption, proprietary-based encryption and blockchain-based network features and features. While proxy encryption and proprietary-based encryption ensures better data access control, network retention provides an effective delivery so that the concept of data-focused communication provides adequate quality in data delivery. Blockchain is designed to prevent high throughput and data sharing and to ensure a secure system of organizations across the network. In our article, the data owner promotes a list of access controls stored in the blockchain. Only authorized users can access the data.

Our system model is shown in the image below introducing a blockchain-based PRE method of data sharing across networks.

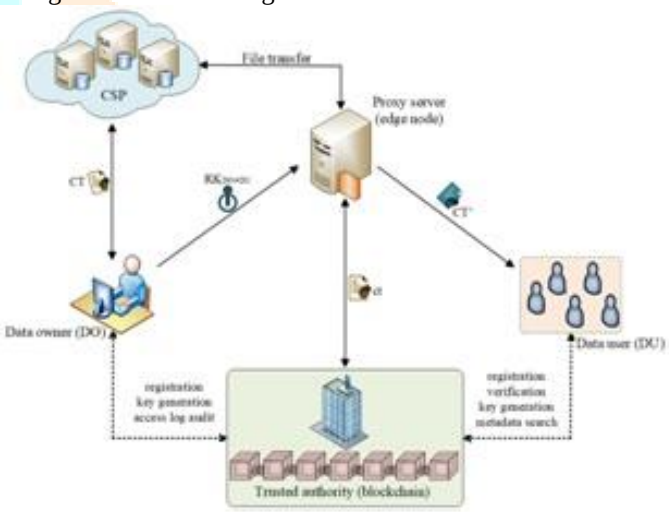

Fig.4 PRE method for blockchain based Data sharing

Edge devices behave as proxy servers and provide the encryption service to the authorized user. When data is cached on peripheral network devices, peripheral devices provide customer service with high availability and performance. Data users retrieve encryption keys from the data owner, extract the ciphertext text from CSP (cloud service provider) and convert the technical text into a data user identifier. It works like a reliable company, but it is a investigative company. Blockchain acts as a TA (Trusted Authorization System Parameters). Through authenticity and transparency, distributed servers provide private TA keys to authenticated users in the network, which increases data privacy and security so that data owners can manage their data. Effectively, it registers the blockchain network and issues membership keys to data owners and data users. When a delegate requests data access, the delegator generates a verified user encryption key using the user ID and IBE.

IV. SYSTEM IMPLEMENTATION:

In this part of paper we provide the workflow of our system and the sequence diagram for data flow in our system.

This article introduces the re-encryption scheme where users are the owners of their data. When data is cached on the network edge device, the edge device serves clients with high availability and performance. The data user receives the re-encryption key from the data owner, extracts the ciphertext from the cloud service provider (CSP), and converts the descriptive text into the data user's identity. We operate as an honest company, but we are a research company. The blockchain acts as a Trusted Authority to Enable System Parameters (TA). Using trust and transparency, distributed ledgers provide TA secret keys to trusted users on the network, enhancing data privacy and security, allowing data owners to control their data. Basically, the blockchain network registers and issues membership keys to data owners and data users. When a data consumer requests access to the data, the owner uses the IBE user ID to generate a verified re-encryption key for the data user. The following sequence diagram illustrates the same.

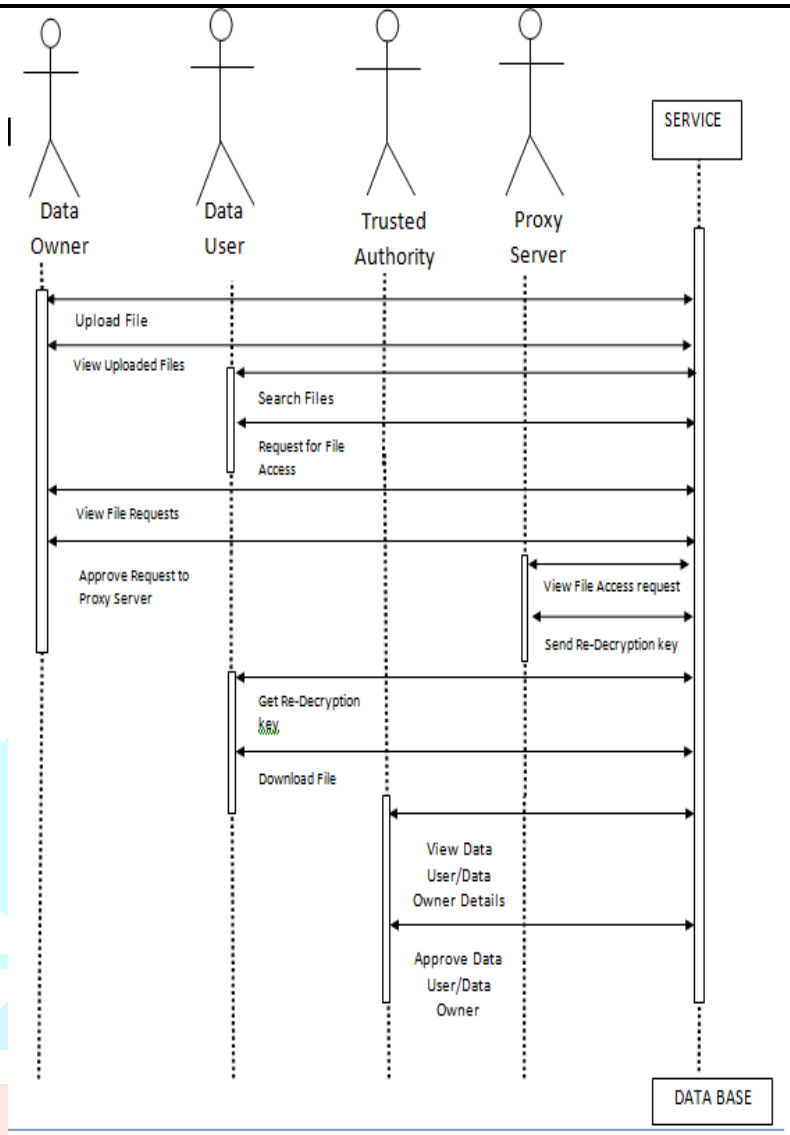

Fig 5: Sequence diagram for Proxy reencryption algorithm based on blockchain.

The proxy reencryption have only four tuples as well as IBE also have only 4 tuples where as our scheme uses combined approach and have six tuples.The algorithm for an Identity-Based Proxy Re-encryption scheme is a seven tuple algorithm defined below:

1. Setup — generates public params and master key by given security input
   - [INPUT] Security Parameter
   - [INPUT] Select random generator g
   - [INPUT] Global Public Parameter
   - [OUTPUT] Pick master key a and set public key pk of PKG:

$$\rho k = g^{\wedge}\alpha, \sigma \epsilon \; Z\_p$$

Pick MK and calculate PKG public Key

2. Key-gen(MK,id) — generates User's secret key by params & existing MK.
   - [INPUT] Identity string id
   - [INPUT] Master Key a
   - [OUTPUT] Private Key sk_{id} for identity id

$$\mathbf{sk_{id} = pk_{id}^{\sigma}\ ,\ pk_{id} = H(id)}$$

Shift id to require group G to get Public key

3. Encryption — sender computes ciphertext from input message m and input identity id on condition r which is pick random here and outputs a second level ciphertext
   - [INPUT] Message m
   - [INPUT] Identity string id
   - [OUTPUT] Pick random r
   - [OUTPUT] Cipher text c = (c1, c2):

$$\mathbf{C_1 = g^{\gamma}\ ,\ C_2 = m.e\ (pk_{id}, pk_{id}), \gamma \varepsilon Z_p}$$

r is used to randomize output

4. Re-KeyGen — To compute new cipher text a new security key is generated.
   - [INPU] Identity strring id
   - [INPUT] a secret key skid
   - [INPUT] Public Parameters params
   - [OUTPUT] the re-encryption key rkID

5. Re-Encryption — A received cipher text is encypted again to provide more security with a new generated re-encryption key rkID
   - [INPUT] re-encryption key rkID
   - [INPUT] a cipher text c
   - [INPUT] identity IDi
   - [OUTPUT] A high quality ciphertext CPK

6. Decryption-Phase1 —The delegate indirectly tries to decrypt CID0 by running Identity based decyption with the first private key skID0 .
   - [INPUT] Private key skID0
   - [INPUT] ciphertext C
   - [INPUT] Identity string id
   - [OUTPUT] First level Cipher Text C

7. Decraytion-Phase2 — To obtain the original message delegate decrypts a message with the help of generated private key.
   - [INPU] Identity strring id
   - [INPUT] a secret key skid
   - [INPUT] Second level cipher text
   - [OUTPT} The mesaage m

Note that our security model uses second level ciphertext to receive original message. For our method we require to apply decryption twice to reach towards original message.

V. PERFORMANCE ANALYSIS:

Our system is more secure. Followinng figure shows a bar chart which showas how much amount of time required for encryption purpose and how much time is required for decryption purpose.

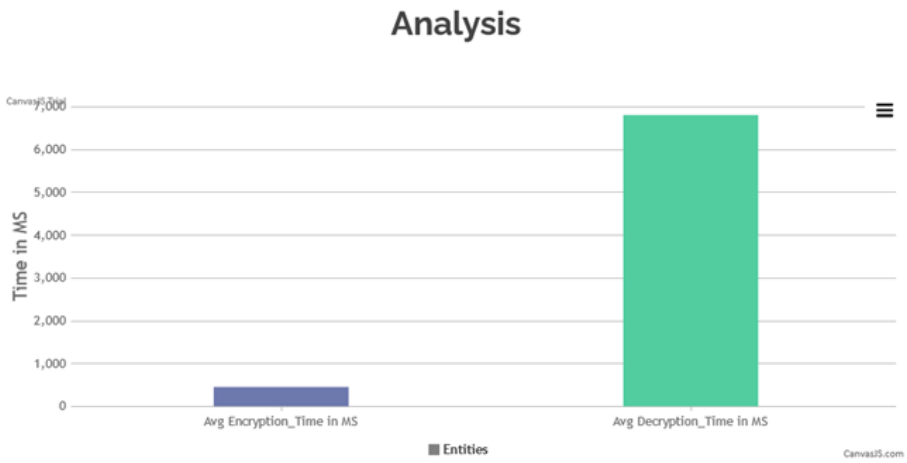

Fig. 6 : Average time of Encryption and Description

Our system is protected from intruder attacks, such attacks may require authentication authority to provide the user with a fake public key. This often leads to the recording of sensitive information. In our system, the blockchain acts as a certificate authority. User community key is located in the block and data is distributed to participating nodes through the front and bottom block links. This renders the public key invalid and makes it difficult for attackers to publish duplicate keys.

When a criminal hits a system, he inserts his own version of the data into the system. There is absolutely no way to ensure that the data has not changed. In contrast, our blockchain-based approach allows us to publish certain data needed to protect each user from fraud.

VI. CONCLUSION:

The paper uses state-of-the-art technology to maximize efficiency and eliminate single points of failure. In addition, because of evidence of disruption and consistent features, blockchain technology improves security and data and uses targeted technologies to increase efficiency and eliminate a single point of failure. In addition, due to evidence of disruption and consistent features, blockchain technology improves data security and integrity.

Data sharing is one of the most popular Internet of Things apps. In the case of cloud computing, a PRE-based data sharing scheme is being developed to ensure data privacy, integrity and confidentiality. IBPRE technology can be used to securely store and distribute encrypted data. Due to limited resources, in-depth calculations can be done with a peripheral device. By integrating ICN features into this strategy, both service level and network bandwidth usage can be improved. We provide a variety of ways for a user to view encrypted data using a blockchain-based system. Improved access controls allow data holders to keep their information private. The analysis and results of our proposed model show how effective it is compared to other methods.

REFRENCES:

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tut., vol. 17, no. 4, pp. 2347–2376, Oct./Dec. 2015.

[2] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 1998, pp. 127–144.

[3] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc.Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984,pp. 47–53.

[4] Agyekum, K. O. B. O., Xia, Q., Sifah, E. B., Cobblah, C. N. A., Xia, H., & Gao, J. (2021). A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain. IEEE Systems Journal.

[5] Fan, Q., Chen, J., Deborah, L. J., & Luo, M. (2021). A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain. Journal of Systems Architecture, 117, 102112.

[6] Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wireless Communications, 25(6), 12-18.

[7] Xuan, S., Zhang, Y., Tang, H., Chung, I., Wang, W., & Yang, W. (2019). Hierarchically authorized transactions for massive internet-of-things data sharing based on multilayer blockchain. Applied Sciences, 9(23), 5159.

[8] Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, 4(3), 149-160.

[9] Viriyasitavat, W., Da Xu, L., Bi, Z., & Hoonsopon, D. (2019). Blockchain technology for applications in internet of things—mapping from system design perspective. IEEE Internet of Things Journal, 6(5), 8155-8168.

[10] G. Manogaran, M. Alazab, P. M. Shakeel and C. -H. Hsu, "Blockchain Assisted Secure Data Sharing Model for Internet of Things Based Smart Industries," in *IEEE Transactions on Reliability*, doi: 10.1109/TR.2020.3047833

[11] H. Xu, Q. He, X. Li, B. Jiang and K. Qin, "BDSS-FA: A Blockchain-Based Data Security Sharing Platform with Fine-Grained Access Control," in *IEEE Access*, vol. 8, pp. 87552-87561, 2020, doi: 10.1109/ACCESS.2020.2992649.

[12] W. Liang, M. Tang, J. Long, X. Peng, J. Xu and K. Li, "A Secure FaBric Blockchain-Based Data Transmission Technique for Industrial Internet-of-Things," in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3582-3592, June 2019, doi: 10.1109/TII.2019.2907092.

[13] J. Lu, J. Shen, P. Vijayakumar and B. B. Gupta, "Blockchain-based Secure Data Storage Protocol for Sensors in the Industrial Internet of Things," in *IEEE Transactions on Industrial Informatics*, doi: 10.1109/TII.2021.3112601.

[14] H. -N. Dai, Z. Zheng and Y. Zhang, "Blockchain for Internet of Things: A Survey," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076-8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.

[15] Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G.B. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. Int. J. Intell. Syst. Appl. 2018, 10, 40–48.

[16] Fernandez-Carames, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. IEEE Access 2018, 6, 32979–33001.

[17] Atlam, H.F.; Wills, G.B. Intersections between IoT and distributed ledger. In Advances in Organometallic Chemistry Volume 60; Elsevier BV: Amsterdam, The Netherlands, 2019; pp. 73–113.

[18] Karafiloski, E.; Mishev, A. Blockchain solutions for big data challenges: A literature review. In Proceedings of the IEEE EUROCON 2017—17th International Conference on Smart Technologies, Ohrid, Macedonia, 6–8 July 2017; pp. 763–768.

[19] Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. 2018, 88, 173–190.

[20] Yin, S.; Lu, Y.; Li, Y. Design and implementation of IoT centralized management model with linkage policy. In Proceedings of the Third International Conference on Cyberspace Technology (CCT 2015), Beijing, China, 17–18 October 2015; pp. 5–9.

[21] Atlam, H.F.; Wills, G.B. IoT Security, Privacy, Safety and Ethics. In Intelligent Sensing, Instrumentation and Measurements; Springer Science and Business Media LLC: Berlin, Germany, 2019; pp. 123–149. 14. Atlam, H.F.; Walters, R.J.; Wills, G.B. Internet of Nano Things. In Proceedings of the 2nd International Conference on Cloud and Big Data Computing (ICCBDC 2018), Barcelona, Spain, 3–5 August 2018; pp. 71–77.

[22] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available online: https://git.dhimmel. com/bitcoin-whitepaper/ (accessed on 13 October 2020).

[23] Honar Pajooh, M Rashid, F Alam, S Demidenko Multi-layer blockchain-based security architecture for internet of things Sensor 772(2021)

[24] Zhang, Q., Li, Y., Wang, R., Liu, L., Tan, Y. A., & Hu, J. (2021). Data security sharing model based on privacy protection for blockchain enabled industrial Internet of Things. International Journal of Intelligent Systems, 36(1), 94-111.

[25] Chi, J., Li, Y., Huang, J., Liu, J., Jin, Y., Chen, C., & Qiu, T. (2020). A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things. Journal of Network and Computer Applications, 167, 102710.

[26] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc.Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984,

[27] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Int. Conf. Theory Appl.Cryptographic Techn., Springer, May 2004, pp. 506–522.