International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Discovering Proxy Re-encryption on Medical IoT data using Blockchain

Shinde Tanmay Balkrushna[1], Dahatonde Mangesh Ramesh[2], Thorat Swastik Jaysing[3],

Prof. A. S. Dumbre[4] , Prof. S. K. Said[5]

[1]Computer dept., Jaihind Collage of Engg. Kuran,Pune
[2] Computer dept., Jaihind Collage of Engg. Kuran,Pune
[3] Computer dept., Jaihind Collage of Engg. Kuran,Pune
[4] Computer dept., Jaihind Collage of Engg. Kuran,Pune
[5] Computer dept., Jaihind Collage of Engg. Kuran,Pune

Abstract - During the process of re-encrypting a ciphertext, proxy re-encryption could hinder a proxy that has not been completely authenticated from receiving any insight into the real plaintext of the data being encrypted. Because of the versatility it provides, proxy re-encryption has become more popular in recent years. It should not come as a surprise that the high level of computationally complexity expenditure makes it difficult to deploy it extensively in functional settings, as determined by performance assessments. The administration of user information must also be delegated to distant cloud infrastructures in order to implement the majority of the following techniques. In the event that the administrators of third-party online storage services are subjected to an assault, sensitive customer data may be put in jeopardy, and it is even possible that it may be deleted entirely. A wide range of researchers arrived across an assortment of strategies for handling security vulnerabilities that crop up in different application scenarios, and these strategies have all been thoroughly evaluated to assist us in arriving at our technique. The objective of the proxy reencryption solution that has been described is to secure IoMT data stored in the cloud through the implementation of a distributed ledger system such as Blockchain. By using a Blockchain distributed structure, the suggested method for proxy reencryption safeguards the data that is stored on a public cloud and corresponds with the Internet of Medical Things. This strategy has been quantified by the execution of extensive experiments, which have resulted in successful results.

Key Words: Search over encrypted data, Cryptography, Medical Health Records, Public Cloud, and Internet of Medical Things.

1.INTRODUCTION

As the information age progresses, the amount of data produced by users also grows exponentially. It's quite evident that the user's local PC memory is insufficient. More and more people are using cloud computing services to archive, process, and administer their data. While there are numerous ways in which cloud-based applications enhance users' lives, these are also significant hazards to users' confidentiality and safety.

When information is uploaded to a remote server, the owner of that data no longer has access to it and must instead depend on the server's ability to perform any required operations. Since then, additional challenges have arisen in cloud data privacy, such as strategies to ensure data privacy and the effectiveness of user restricted access and authorization management.

Most modern cloud storage systems, on the other hand, have a centralized structure, meaning that data administration is controlled by a single entity. There are significant distribution expenses as well as computation charges when using this approach. Subsequently is essential to provide a reliable, safe, and efficient method of collaborating on cloud storage. An authorization method based on cloud ciphertext is proposed as a means of ensuring the security of sensitive information. By encoding the data with a key and storing the message with encryption in the cloud, confidentiality is ensured. The data owner also has authority over the user's key and, by extension, their access rights.

Traditional studies advocate for a participation method of encryption that uses the function as a decryption criteria. One possible solution to this problem is to build an integrated cloud re-encryption data exchange architecture on top of attribute cryptography. This method not only makes it easier for data owners to handle their data, but it also allows for more flexible ciphertext management of identities. We provide a smart and flexible method of proxy re-encryption. By granting the authorized user the ability to decrypt any re-encrypted ciphertext employing the user's component, the information proprietor can offer accessibility to the plaintext message. Afterwards, it was proposed that a proxy reencryption mechanism benefit from including elements of distinctiveness, credentials, and environment.

While the above measures take reasonable precautions to protect sensitive data, they do nothing to help users quickly access the specific data and knowledge they need as part of the data sharing process. To improve access performance during the exchange of data, we present a distinctive proxy re-encryption mechanism that makes use of cryptographically indexed phrases. Nevertheless, this approach cannot be used to

develop a ciphertext decryption algorithm suitable for real-world use. The existing literature addresses this issue by using a key-based characteristic proxy re-encryption methodology to improve keyword search, and has shown the effectiveness of this method inside a randomized oracle paradigm.

However, performance evaluations show that the technique is too computationally complicated to be widely implemented. The bulk of these techniques include sending user data to a third-party cloud service for management. Critical client data may be jeopardized or even wiped permanently if the management teams of third-party cloud solutions are attacked.

The advent of Blockchain technology has led to a communally governed, decentralized, tamper-proof, unforgeable, and transparent form of management. Blockchain is only a decentralized database that we already own. Furthermore, the fundamental technology behind Bitcoin is a chain of encrypted data chunks. The blocks that appear on the Cryptocurrency blockchain are collections of related transactions. Information required to construct a new block and guarantee the validity of the information contained in the preceding one. To start with, one of the primary benefits of the blockchain is that it is decentralized. The distributed ledger eliminates the need for trusted third parties or dedicated hardware servers. Blockchain is self-sufficient because transactions do not need to go via a central server. Networks provide the self-verification, transfer, and management of data. The distributed nature of the Blockchain is its fundamental selling point. In addition to all of this, the Blockchain is also private, secure, readily available and decentralized.

For single-hop bidirectional proxy re-encryption schemes with delegable authenticity, Yu Zhan [1] presents a safe paradigm against ciphertext attacks and builds a concrete implementation. The authors address the issue of re-encryption by an adversary by using the Gap-Diffie-Hellman brief verification technique. This technique has been shown safe against ciphertext assaults by vulnerability assessment. As a result, the issue raised in the introduction is addressed in this work. In addition, the scheme's computational challenge is analyzed and compared to that of other systems. It's worth noting that the authors' method for creating a publicly verifiable proxy re-encryption strategy may be employed in any publicly verifiable proxy re-encryption methodology. This broadens the practical applicability of proxy reencryption techniques.

According to Zhanwen Chen [2], cloud computing has become an integral part of our everyday lives, making it easier to store and share data in a variety of settings, including professional and personal interactions. However, there is rising awareness regarding cloud data security. There are still limitations to preexisting methods that aim to address such issues. Some don't allow for user-specific customization, while others have a convoluted encryption procedure and restrict your ability to choose your intended audience. In this study, the authors describe a novel strategy for unconditional proxy broadcasting re-encryption techniques that allows for adaptive in-system user configuration and the targeted user organization.

Two safe and non-intrusive synchronous deep learning methods are proposed by Xiaoyu Zhang [3]. The identical framework may be trained in parallel and sequentially across multiple consumers, all while protecting the privacy of the users' data that is entered. DeepPAR relies on proxy re-encryption to preserve the confidentiality of the regulations while safeguarding the anonymity of the inputs of the many stakeholders. Furthermore, the group key management architecture upon which DeepDPA is based ensures that its minimal flexible involvement notification is only impacted by its closest neighboring neighbors. In addition, DeepDPA allows for dynamic privacy-preserving machine learning to be used in retroactive situations.

Section 2 of this research article presents an analysis of the relevant literature; Section 3 explains the research approach; Section 4 discusses the experimental assessments; and Section 5 closes with suggestions for further study in the future.

2. RELATED WORKS

Yi-Fan Tseng [4] provides a novel general structure for deriving a single-hop unidirectional conceptual proxy key re-encapsulation method from an incremental boolean key simplification approach. Combining with a reliable encrypted symmetric key allows for a single-hop unidirectional unconditional proxy re-encryption procedure. The solution provides a fresh strategy for developing a semantically sound proxy re-encryption that is compatible with all predicated operations, solving the problem that the currently available criterion proxy re-encryption only supports the kernel-specific criteria functionality.

It has been proved that our technique is selected plaintext private dependable in the stochastic oracle situation, as specified by Chunpeng Ge [5], and an actual application under this requirement has been demonstrated. The cost-effectiveness and practicality of their solution is shown by a comparison of its attributes and performance. Key termination for a data-sensitive

infrastructure in a cloud-based setting, for example a volunteer-based genetic investigation, may be gracefully handled using the reversible identity-based broadcasting proxy reconfiguration approach. This study has helped shed light on the problem of suspended keys for information collaborating, but it has also raised some fascinating open questions, such as how to provide more creativity on recognition and how to construct an irrevocable identity-based communication proxy re-encryption approach that makes use of arbitrary oracles.

Khaled Rabieh [6] offered a secure but efficient dissemination mechanism to guarantee that outside applicants as emergency personnel might have instantaneous or future knowledge of videos shot by uavs without risking the secrecy of the content. Because these movies have been encrypted and kept in the cloud, user confidentiality is not compromised while they are viewing them. The original secret key used to encrypt drone video is never shared with rescue workers for privacy and security concerns. Re-encryption may also be accomplished via the cloud server's Command Center by using a proxy re-encryption. A fresh encryption key is generated and stored in the cloud in order to kick off the process of re-encryption. The authors built a functional model using a virtual environment and the OpenCV library.

According to Koushik Bhargav Muthe's [7] blueprint for the Internet's next iteration, Web 3.0, it is possible for all humans to function as a single, interconnected organism thanks to the Internet's decentralized architecture. The current situation of the internet was assessed, and a plan for its complete decentralization was proposed in this paper. Since the proposed Decentranet approach remains in the evidence of concept stage, it can only be used for research purposes at this time. Scalability is a production issue because of the current Network's inadequacies. In order to further develop the system, it is necessary to pique the attention of the mediators. Ethereum 1.0, on which the current protocol is built, uses an agreement technique that utilizes Evidence of Work, that isn't ideal for completely decentralized applications.

Yanfang Lei [8] uses proxy re-encryption technology and Blockchains to design a system for retrieving information that can be used to change who has access to information stored in the public cloud and when. The scenario is first introduced to the audience with some background information. Second, the approach's philosophy and structure of the system are described in great detail. Next, we examine the reliability and safety of the strategy. Numerical experiments are then used to evaluate the algorithm's performance and study the scheme's functionality. One advantage of this method is that it may drastically reduce the likelihood of informational collaboration by means of ciphertext separation and maintenance. However, the goal of a probabilistic authentication improvement is best realized if the main settings of the proxy re-encryption are genuinely only adjusted once the access rights are amended.

Mazhar Ali [9] developed a method for securely storing and transmitting PHRs to the proper people in the cloud. By implementing fine-grained, patient-centric restrictions over who gets a glimpse of which aspects of confidential health data, this method assures that such data remains private and safe. The authors guarantee that no authorized network administrators will get unauthorized possession of confidential medical data by developing a fine-grained accessibility management mechanism. Ownership of safeguarded medical information encrypts and stores their data in the cloud, where it is accessible only to individuals who have been given the correct re-encryption keys through a semi-trusted proxy. The semi-trusted proxy will generate and save pairs of both public and private keys for clients within the framework of the system. Conversely, it controls both backward and forward authentication for persons entering and departing the framework, as well as patient confidentiality and the protection of health information.

Di Wang [10] proposed an innovative approach of reliable data sharing and individualized vendors for infrastructure engineering based on blockchain technology for the consortium to address the disadvantage inherent in traditional smart transportation's centralized management of information and to concentrate on guaranteeing confidentiality and reliability in the information involvement procedure. The proposed policy characteristic based proxy re-encryption approach allows for secure data interchange and the avoidance of on-board component confidentiality breaches by dividing the key across between the characteristic key and the query key. In the future, the smart contract might be employed in the tourism industry to provide precise and customized amenities like insurance quotations and vehicle maintenance. The security analysis and assessment of

performance demonstrate the approach's strong advantages with regard to of privacy, efficiency, cost, and responsiveness.

Ammar Ayman Battah [11] proposed a fully decentralized blockchain-based multi-party authorisation system to guarantee the permanence, transparency credibility, and integrity of log entries relating to access/permissions. It has been suggested that a communal and autonomous storage system, such an interplanetary directory system, might enable utilization of safeguarded data that is shared by proxy re-encryption with numerous oracles. The proposed smart contracts were developed by the academics, and they include relational mechanisms that give oracles ratings based on their history of good and bad deeds. Researchers utilized Ethereum smart contracts to build the protocols, parameters, and incidents. The smart contract solution is available on GitHub, and it can be easily adapted to run across either permissionless as well as anonymized public blockchains to meet the needs of different industries. The researchers described how they came up with, tested, and confirmed the algorithms and other components of the overall system.

Shunrong Jiang [12] exposes the security issues when employing designated Information Networking towards Vehicular Ad Hoc Systems and recommends suitable approaches, such as reliable and safe access management, to address these concerns and enable the provision of efficient and personal safety regulates for dissemination of media in Vehicular Named Data Networking. To get started, the researchers build a proxy re-encryption mechanism that can perform authentication management, cancellation, and upgrading even in absence of a trusted source. In order to tackle the issue of anonymized verification and integrity verification, researchers employ aliases and an identifier-based verification. Researchers offer a system of incentives based on a hashed certification to guarantee Designated Data Networking's use in Vehicular Ad Hoc Systems. The security analysis found that well-implemented controls on access might provide a sufficient degree of safety for VNDN deployments. Further, the results of the simulations show that the proposed secure technique has almost little effect on the performance of the network.

3. PROPOSED METHODOLGY

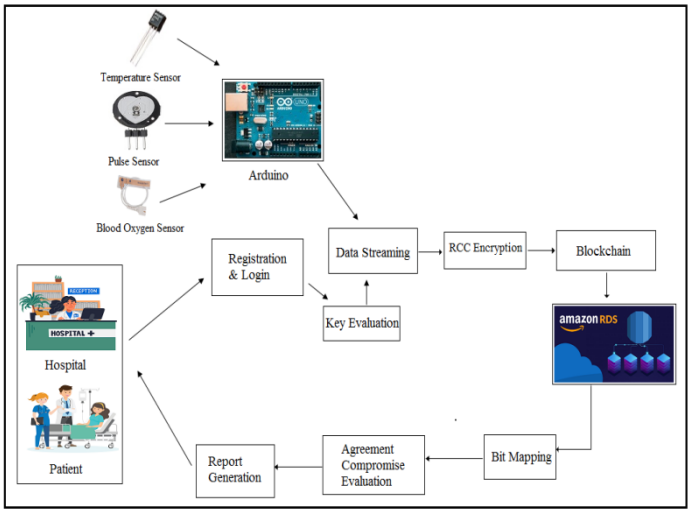

Fig-1: Proposed Methodology

The proposed approach for the purpose of achieving secure medical sensor data through proxy reencryption on the public cloud have been realized through blockchain which has been depicted in the figure 1 above and the steps taken to achieve this system are elaborated below.

Step 1: Admin Registration and Login– The provided method features a sleek graphical user interface that was created using the Java swings framework. The administrator may use this dynamic interface to log in to the system and carry out the many procedures required by this approach. If this is the first time the administrator has visited the site, he or she may register for an account. The sign up form requires details that includes name, email id, mobile number, qualification, registration number, specialty, and years of experience, username and password. This information must be confirmed before an account can be created and the administrator granted access.

The administrator assigns a specific user ID and password for authentication reasons. The admin's operation frame will load after verification. Within this operation window, the administrator may carry out a variety of tasks.

Managing one's profile in the operation frame includes the opportunity to alter the existing password. Login credentials are stored in a database managed by the cloud service provider (AWS or Amazon Web Services in this example). The cloud is used for the authentication of the administrator and the storing of the

login information (username and password). Consequently, the cloud database is also used for the manage profile function, which modifies the user's profile characteristics.

The administrator may enter the data storage option to start the data streaming from the IoT sensors. The data from the sensors will be gathered using a submenu called "data streaming" in the "data storage" menu. After deciding to stream data, the user is sent to a new screen where they may either begin streaming immediately or pause streaming at any time. When you select the start streaming alternative, the sensors will begin sending data, and when you hit the stop streaming option, the data will cease being transmitted. In the following stage of the process, we'll talk about the data arriving in from the sensors.

Step 2: Sensor Data Streaming – The first step in obtaining data from sensors is to initiate a data stream. As soon as the user hits the button to begin streaming data, the sensor readings will be collected. Connecting the Arduino UNO microcontroller to the development platform PC is the fundamental step. An Arduino UNO microcontroller is being utilized for sensor integration and data collection. Multiple sensors are used in this setup, some of which may detect changes in body temperature and pulse rate. Similar sensors are attached to an Arduino microcontroller and instructed to send readings to a laptop.

The microcontroller's sensor readings are collected, and the Java program is launched. To achieve this, a simple graphical user interface (GUI) has been designed to initiate the process of gathering sensor data. Selecting this setting initiates a background thread that monitors the COM4 port for sensor readings. Using the current time and date, the thread records data from sensors such as a heart rate tracker and temperature monitor. As long as the thread is active, it will keep going. The user can tap the stop button on the interface in order to quickly interrupt the thread and hence the acquisition of sensor data.

Step 3: Sensor Data Encryption and Cloud Storage – In this step, the received sensor data from the previous phase is utilized as an input, together with the current time and date. This is precisely why encryption keys are generated using the Reverse circular Cipher Encryption procedure.

For safety reasons, the code uses a built-in symmetric encryption key. By providing this key to the RCC procedure, additional keys may be produced and utilized to protect the anonymity of the sensors. In order to encrypt the data, the acquired sensor values are sent to the Reverse Circle Cipher method, which executes as shown below.

Reverse Circle Cipher – When used with a cloud service, the Reverse Circle Cipher is one of several very effective cryptographic algorithms that may be employed. The RCC technique involves exchanging inbound characters after first rotating them precisely anti-clockwise or clockwise. To accomplish this, the described approach segments sensor data before rotating each section to encode its information. The Reverse Circle Cipher successfully encrypts the data, which is subsequently sent to a server in the cloud. The Reverse Circle Cipher is a strong competitor when it comes to securely encrypting confidential data. It is all established down in Algorithm 1 below for Reverse Circle Cipher Encryption.

ALGORITHM 1: Reverse Circle Cipher

```
// Input: Sensor Data S_D
// Output: Sensor Cipher Data S_CD
Function reverseCircleCipher (S_D, KEY)
1:  Start
2:    Initialize list Block LST_BLK =∅, DIV_STR="", addupval=0
3:      for i = 0 to size of KEY
4:            addupval= addupval+ASCII (KEY_[i])
5:      end for

6:      addupval= addupval MOD 20

7:      for i = 0 to size of S_D
8:            char ch= S_D[i]
9:            D_STR = D_STR +ch
10:       if (D_STR size =10), then
11:          LST_BLK = LST_BLK + D_STR
12:          D_STR =""
13:       end if
14:     end for

15:          LST_BLK = LST_BLK + D_STR
16:

17:     For i = 0 to size of LST_BLK
```

18: STR= $LST_{BLK\ [i]}$

19: STR=rotate (STR, i)

20: **For** j = 0 to size of STR

21: char ch= $STR_{[j]}$

22: newchar=ASCII(ch) + addupval

23: $S_{CD} = S_{CD} +$newchar

24: ***end for***
25: ***end for***
26: ***return*** S_{CD}
27: **STOP**

Step 4: Blockchain Formation – The data collected by the sensors must be protected before being sent to the cloud. Because of this need, the Blockchain was established. The sensor data and the current time are hashed using the SHA256 algorithm to get the key. To generate a shorter key, the mod operation discards the first seven characters of the long key generated in this manner at random. Due to its prominence, this key is frequently referred to as the Head Key. The key generation process is given in Algorithm 1.

Algorithm 1: Block Head Key Generation

// Input: Sensor Readings with Date and Time SR_{DT}

// Output: Head Key H_K

Function: headKeyGenerator (SR_{DT})

0: Start

1: H_K =Ø

2: SH_{KEY}=*SHA256 (*SR_{DT}*)*

3: N=SH_{KEY} MOD 7

4: ***If*** N<7, ***then***

5: P=N+1

6: ***for*** i=0 **to** H_K length < 7

7: i=i+P

8: ***if i*** < H_K length, ***then***

9: $H_K = H_K + SH_K$ [i]

10: $SH_K =$ rotate (SH_K)

11: ***end if***

12: ***else***

13: i=0

14: ***end for***

15: e***nd if***

16: **return** H_K

17: Stop

Head keys for subsequent transactions are generated using SHA256, with identical parameters computed and appended to the preceding transaction's head key at each iteration of the sensor data streaming. This is done each time data is gathered from sensors and uploaded to the cloud, and the final step is safeguarded by a master key that is maintained in a safe location.

After the information has been added to the blockchain, it is uploaded to Amazon's cloud storage system via the AWS (Amazon Web Services) user interface. In order to do this, select the "create table in cloud" option, and a fresh table will be established in your MySQL database on Amazon's web services. This table stores the encrypted readings from the sensors and provides access to them through the view history menu item in the data storage user interface. The sensor values are encrypted, but the user may decrypt them using the appropriate key to view the sensor readings

4. RESULT AND DISCUSSIONS

The proposed technique for proxy reencryption of sensor data in the public cloud is built in Java through using NetBeans Integrated Development Environment. This approach works best on a Windows laptop equipped with an Intel Core i5 CPU, 8 GB of RAM, and 1 TB of storage space. The various sensors are transmitting their data to the Arduino UNO microcontroller. Amazon S3 is being used as the cloud database to store the sensor data.

The proposed method's viability has been carefully examined. The section below contains the experimental study's findings.

Encryption and Decryption Time performance

The suggested approach makes use of encryption and decryption techniques in order to guarantee that the sensor values will maintain their confidentiality while being sent to the cloud database. If one observes the methods outlined in this part, one will be able to evaluate the efficiency of this technique. Table 1 provides a breakdown, by increasing the number of characters in each turn, for calculating the amount of time consumed encrypting and decrypting data using the RCC approach. This information is presented in a table format in the table 1 below.

Number of Characters	Encryption Time in Milliseconds	Decryption Time in Milliseconds
15	3	3
1808	15	17
2808	33	32
3012	46	54
5003	52	56
5789	64	62
6342	67	64
8426	77	78
9210	82	81
9991	96	99

Table 1: Encryption and Decryption time performance

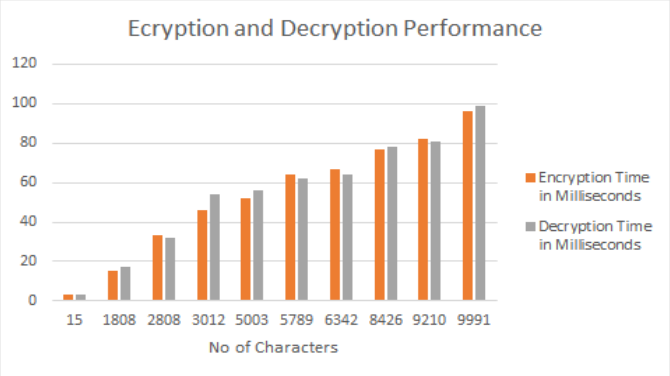

Fig 3: Encryption and Decryption Time

The bar graph representation shown above in Figure 3 is suitable for use in conducting a visual examination of the data that has been supplied in table 1 above. It is abundantly clear that the amount of time necessary to encrypt and decode is not proportional to the number of characters that are entered. This is because the type of encryption used for this approach, the reverse circle cipher, has been the subject of a significant amount of research and has also been put to use in this methodology very accurately. Because of this, the results of the experimentation suggest that the strategy is being carried out in a rather satisfactory manner.

5. CONCLUSIONS

Proxy re-encryption may prohibit a proxy that cannot be entirely authorized from gaining any insight into the actual plaintext whilst re-encrypting a ciphertext. Proxy re-encryption has seen widespread application due to the flexibility it affords. Unsurprisingly, the computational complexity overhead renders it impossible for extensive operational implementation, as per performance benchmarks. The bulk of the following strategies also require delegating the management of user information to remote cloud infrastructures. In the case of an attack on the operators of third-party cloud storage, critical client data may be jeopardized or possibly even wiped permanently. Diverse academics came up with numerous approaches to deal with the security breaches that spring up in various application contexts, and they have all been properly assessed to help us arrive at our strategy. Protecting IoMT data in the cloud using a distributed ledger like Blockchain is the goal of the suggested proxy re-encryption method.

In the future the proposed approach can be enhanced to work in the direction of creating the application for hospitals to store the Medical IOT data.

REFERENCES

[1] Y. Zhan et al., "Improved Proxy Re-Encryption With Delegatable Verifiability," in IEEE Systems Journal, vol. 14, no. 1, pp. 592-602, March 2020, doi: 10.1109/JSYST.2019.2911556.

[2] Z. Chen, J. Chen and W. Meng, "A New Dynamic Conditional Proxy Broadcast Re-Encryption Scheme for Cloud Storage and Sharing," 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 2020, pp. 569-576, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00101.

[3] X. Zhang, X. Chen, J. K. Liu and Y. Xiang, "DeepPAR and DeepDPA: Privacy Preserving and Asynchronous Deep Learning for Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2081-2090, March 2020, doi: 10.1109/TII.2019.2941244.

[4] Y. -F. Tseng, Z. -Y. Liu and R. Tso, "A Generic Construction of Predicate Proxy Key Re-encapsulation Mechanism," 2020 15th Asia Joint Conference on Information Security (AsiaJCIS), 2020, pp. 1-8, doi: 10.1109/AsiaJCIS50894.2020.00013.

[5] C. Ge, Z. Liu, J. Xia and L. Fang, "Revocable Identity-Based Broadcast Proxy Re-Encryption for Data Sharing in Clouds," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1214-1226, 1 May-June 2021, doi: 10.1109/TDSC.2019.2899300.

[6] K. Rabieh, S. Mercan, K. Akkaya, V. Baboolal and R. S. Aygun, "Privacy-Preserving and Efficient Sharing of Drone Videos in Public Safety Scenarios using Proxy Re-encryption," 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), 2020, pp. 45-52, doi: 10.1109/IRI49571.2020.00015.

[7] K. B. Muthe, T. S. T. Vemuru, K. Sharma and N. S. Mohammad, "Decentranet - An Ethereum, Proxy Re-Encryption and IPFS Based Decentralized Internet," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1-5, doi: 10.1109/ICCCNT49239.2020.9225483.

[8] Y. Lei, Z. Jia, Y. Yang, Y. Cheng and J. Fu, "A Cloud Data Access Authorization Update Scheme Based on Blockchain," 2020 3rd International Conference on Smart BlockChain (SmartBlock), 2020, pp. 33-38, doi: 10.1109/SmartBlock52591.2020.00014.

[9] M. Ali, A. Abbas, M. U. S. Khan and S. U. Khan, "SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud," in IEEE Transactions on Cloud Computing, vol. 9, no. 1, pp. 347-359, 1 Jan.-March 2021, doi: 10.1109/TCC.2018.2854790.

[10] D. Wang and X. Zhang, "Secure Data Sharing and Customized Services for Intelligent Transportation Based on a Consortium Blockchain," in IEEE Access, vol. 8, pp. 56045-56059, 2020, doi: 10.1109/ACCESS.2020.2981945.

[11] A. A. Battah, M. M. Madine, H. Alzaabi, I. Yaqoob, K. Salah and R. Jayaraman, "Blockchain-Based Multi-Party Authorization for Accessing IPFS Encrypted Data," in IEEE Access, vol. 8, pp. 196813-196825, 2020, doi: 10.1109/ACCESS.2020.3034260.

[12] S. Jiang, J. Liu, L. Wang, Y. Zhou and Y. Fang, "ESAC: An Efficient and Secure Access Control Scheme in Vehicular Named Data Networking," in IEEE Transactions on Vehicular Technology, vol. 69, no. 9, pp. 10252-10263, Sept. 2020, doi: 10.1109/TVT.2020.3004459.