IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 10, October 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 10, October 2023 ||

| DOI:10.15680/IJIRSET.2023.1210032 |

Protecting IOT Data with Blockchain and Proxy Re-Encryption: A Dynamic Key Solution

Fathima M, Dr. Safia Naveed. S M.E., Ph.D

P.G. Student, Department of Computer Engineering, KCG College of Technology, Chennai, TN, India

Professor, Department of Computer Engineering, KCG College of Technology, Chennai, TN, India

ABSTRACT: Data sharing is now a prominent feature of cloud-based applications thanks to the growth of the Web and the Internet of Things (IoT). Despite its potential, data security remains a critical concern due to the potential misuse of sensitive information. This article offers a novel approach to safeguarding Proxy re-encryption is used for data exchange in cloud environments. Identity-Based Encryption (IBE) enables owners of encrypted data to safely transfer that data to the cloud. Proxy re-encryption is used to allow authorized people to access the data. Due to the resource limitations of IoT devices effectively managing computationally heavy activities, an edge device behaves like a proxy server. Leveraging information-centric networking features, cached content is delivered effectively through the proxy, enhancing service quality and optimizing network bandwidth utilization. Moreover, our system architecture incorporates blockchain technology, a disruptive innovation fostering data sharing that is decentralized. With this approach, centralized systems' bottlenecks are removed & establish data access control at the granular level. The success of our plan in maintaining data confidentiality, integrity, & overall security has been confirmed by thorough security analyses and evaluations. This integrated solution addresses critical concerns surrounding data security in IoT-driven cloud environments, paving the way for more robust and trustworthy data sharing practices.

KEYWORDS : Data Security, Internet of Things (IoT), Blockchain, Proxy Re-Encryption (PRE)

I. INTRODUCTION

The rapid development of of Internet of Things (IoT) has propelled data sharing to the forefront of cloud computing applications, marking a transformative era in information exchange. Yet, amidst the promise and potential, a paramount concern looms large: the security of shared data. As the volume of sensitive information escalates, the risks of unauthorized access and misuse become increasingly pronounced. In response, this article introduces a pioneering solution that harnesses the power of strengthening data sharing across cloud settings using proxy re-encryption.

Fundamentally, this approach enables data owners to employ identity-based encryption to safely entrust their encrypted information to the cloud. A major development which renders it safe for some users to view the data is proxy re-encryption ensuring that only those with explicit authorization may retrieve and utilize the information. Recognizing the constraints faced by Internet of Things (IoT) devices, we employ a proxy server on an edge device, strategically positioned to efficiently manage computational tasks that may otherwise overwhelm these resource-limited devices. Furthermore, our approach leverages the advanced capabilities of information-centric networking, streamlining the delivery of cached content through the proxy. This optimization not only enhances the quality of service but also maximizes the utilization of network bandwidth, ensuring a seamless and efficient data sharing experience.

In addition to these cutting-edge techniques, our system architecture incorporates the disruptive potential of blockchain technology. This paradigm-shifting innovation decentralizes data sharing, eliminating the bottlenecks associated with traditional centralized systems. Furthermore, it establishes meticulous fine-grained access controls, allowing for a more nuanced and customized approach to data security.

Rigorous security analyses and comprehensive evaluations affirm the potency of our plan in preserving data privacy, consistency, and overall security. By integrating these components, our solution confronts the critical challenges surrounding data security in IoT-driven cloud environments head-on. This holistic approach sets the stage for a future characterized by robust, trustworthy, and resilient data sharing practices, poised to redefine the landscape of information exchange in the digital age.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 10, October 2023 ||

| DOI:10.15680/IJIRSET.2023.1210032 |

II. LITERATURE SURVEY

Key-policy ABE (KP-ABE) & PRE were coupled by Yu et al. [1] to provide a suggestion for a cloud data sharing system. The data was encrypted using KP-ABE, making decryption possible only with the correct combination of attribute keys that are secret. The internet managed all attribute secret keys, with the possible exception of one special private key for user revocation, in along with managing the encrypted data. The information that was encrypted had to be re-encrypted when users were revoked since new the data owner must furnish the remaining users with their keys. Despite being effective, the scheme's security was compromised since the re-encryption was carried out carelessly. In order to prevent collaboration involving the service provider as well as users who had their access revoked, Park [2] modified the approach in. Their plan essentially consisted of substituting a reliable third party for the service provider, which suggests that a higher level of trust should be assumed. Similar methods were used by other techniques [3]–[4], Instead of using secret keys, they employed ciphertext-policy ABE (CP-ABE), which links the access policy to the ciphertext.

Liu et al. [5] also suggested a time-restricted restriction of access technique based on PRE and ABE. ABE was used to create time-based access control policies, whereas PRE was employed to update time-based characteristics. Despite the advantages of these techniques, the IoT cannot employ them due to their high computing costs for encryption & decryption. Han et al. introduced an IBE PRE technique appropriate for data exchange in [6]. The re-encryption key was linked to a particular ciphertext in addition to the identities of the users. This suggested that each combination of data users and shared files required the data owner to generate a unique reencryption key. Lin et al. [7] made a similar suggestion, although they employed a hierarchical PRE as opposed to an identity-based PRE. When various and sophisticated data pieces are taken into account, these two techniques frequently prove to be ineffective. Zhou et al. in [8] presented a combination of PRE and identity-based broadcasting encryption (IBBE) for data sharing. Their goal was to combine two different protocols in a way that allowed conversion without revealing any sensitive information. Agyekum et al., A proxy re-encryption method to secure transmission of data in the Internet of Things using blockchain 1687 was created by Wang et al. [9] in addition to the identity-based PRE (IBPRE) scheme of obtaining medical information. Large-scale access control was made possible by the plan. If a proxy obtains the data owner's re-encryption key, either the intended users can have access to all of the decrypted ciphertexts or none at all.

A condition-based IBE PRE scheme was presented by Shao et al. [10] in response to this. According to their suggestion, the proxy might convert a portion of ciphertexts belonging to one identity into ciphertexts belonging to another identity. It was impossible to grant a set of users the ability to decrypt data, though. Along with the aforementioned, PRE-has been used to reduce security risks associated with IoT [11]; Zyskind et al. [12] leveraged blockchain to facilitate distributed private information management while maintaining privacy; as well as PRE-has been used to reduce security risks associated with IoT [13]. Because the blockchain served as an independent access control manager, no outside party was required. A hash table that was distributed was utilized to implement the data storage, and only the data value was kept on the blockchain. This decreased the danger data leaking. However, their plan did not offer any particular access control paradigm. A chain-based access control approach was developed by Maesa et al. [13] in which the data owner creates policies for the data & stores it on the blockchain. Then, the users are given access rights based on the policies. A comparable solution, created by Fan et al. [14], involves uploading encrypted data to the cloud & storing access control policies as transactions on the blockchain. The usage of public blockchains, which are open to everyone, results in a leakage of access rules despite the fact that these two schemes accomplish tamper-proof systems and simple audits.

Singh and Kim [15] suggested a blockchain-based approach to data exchange in transportation networks that also permits secure vehicle communication. However, the use of an open blockchain does not work effectively for peer-to-peer (P2P) data transmission among vehicles because of the significant cost involved in establishing a freely accessible blockchain inside resource-constrained vehicles. Several centralized & decentralized access control strategies have been suggested in the literature to regulate content in ICN systems. A proxy server and an ABE scheme were used in Silva and Zorzo's [16] access management system for identified data networking. The data owners encrypt the content & create rules of access that ties it before it is published. While the server is where the access rule is kept, encrypted information is kept in the nearby routers. In order to access material, a user first retrieves it from the router, then gets the restriction on access from a proxy server, & finally decrypts the data. Their system allows for user revocation, but because a proxy server is involved in each content access, it has just one point of failure if the proxy server stops functioning. Li et al. [17] developed a privacy-enhancing method for access control in ICN using ABE, where characteristics are handled by a dependable third party. According to the characteristics provided by the third party, a

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 10, October 2023 ||

| DOI:10.15680/IJIRSET.2023.1210032 |

content publisher develops an access policy and encrypts the material using a random asymmetric key. The publisher then hides the random key and the access policy inside the article's name to prevent unauthorized people from viewing the content.

Research Gap

The reviewed literature highlights various approaches in securing data sharing, employing a combination of techniques like Proxy Re-Encryption (PRE), Attribute-Based Encryption (ABE), and blockchain technology. Each approach exhibits distinct strengths and weaknesses. For instance, some schemes introduce potential computational intensity concerns in IoT contexts, while others rely on trusted third parties, implying stronger trust assumptions. Additionally, schemes utilizing public blockchains may inadvertently leak access policies. Moreover, certain proposals face challenges related to potential single points of failure. Addressing these gaps is crucial in devising a tailored and comprehensive solution for secure data sharing in the dynamic landscape of IoT environments.

III. METHODOLOGY

A. *Blockchain*

Fig. 1 below displays Blockchain technology, a sophisticated database system, permits open information exchange inside a business network. In a blockchain database, data is saved in blocks that are linked to one another via chains. The data is still constant in time since the chain cannot be deleted or changed without network agreement. You may set up an unchangeable or irreversible ledger using blockchain technology to manage purchases, payments, accounts, and many other transactions. The system's built-in capabilities, which also prevent unauthorized transaction submissions, make it possible to see these transactions as a whole.

Blockchain constitutes a distributed database that records trades between various nodes, or computers. It offers the foundational technology for virtual currencies like Bitcoin, but its potential applications go beyond these. Fundamentally, a blockchain is composed of a number of blocks of data, each of which has a list of occurrences. By connecting these blocks with cryptographic hashes, a visible and immutable record of every one of the transaction that took place is produced. It becomes very difficult to add or delete a block from the chain after it has been added, offering an elevated degree of security & integrity. Decentralization decreases the need for middlemen, lowers the possibility of fraud, and fosters greater participant trust.

Blockchain, though, is not without problems. For wider use, concerns including scalability, energy use, and regulatory frameworks must be resolved. Nonetheless, the potential benefits offered by blockchain technology continue to drive innovation and exploration in various fields, paving the way for a more decentralized and secure future.

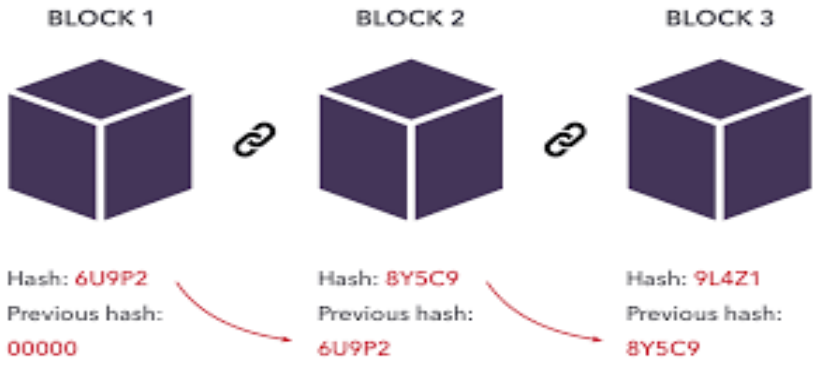

Fig1: Structure of Blockchain

B. *Hashing*

Clients may employ cryptosystem to encrypt the files in the cloud to lowering the threat associated with cloud storing. By maintaining a brief hashing in internal space, the use of a hash value is a suitable method for maintaining data fidelity. By re-tallying up the hashes of the information that was obtained and comparing it to locally preserved information, the server answers are authenticated in this way. Here, we are using MD5 hashing function for security purpose when file uploading and downloading is performed. You can find an illustration of this process in Figure 2.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 10, October 2023 ||

| DOI:10.15680/IJIRSET.2023.1210032 |

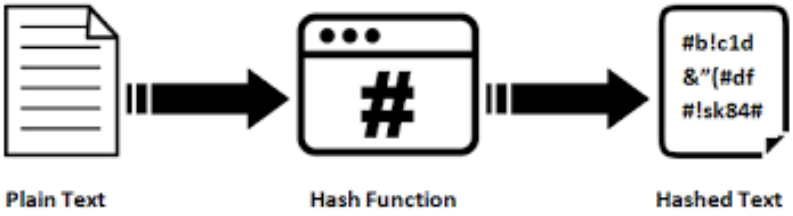

Fig2: Hashing Algorithm

We face issues with information protection, system files, recoveries, network congestion, and hosting safety in CCT.

C. Block Verification Process in Blockchain

The block verification process in blockchain involves using hashing techniques to ensure the integrity and authenticity of data within a block. Here's a brief description of the process:

- **Data Compilation**: A block contains a collection of data, such as transactions or records that need to be verified. This data is compiled together before the verification process begins.
- **Hashing:** The block's data is then fed through a cryptographic hash function, which generates a unique fixed-length string of characters called a hash. The hash is essentially a digital signature of the information in the block.
- **Hash Linking:** The blockchain's previous block's hash is also included in each block. This creates a chain-like structure where each block is linked to the one before it, forming a tamper-evident sequence.
- **Verification:** The generated hash is compared to the hash stored in the previous block. If they match, it confirms that the data within the block has not been altered. Any modification to the data would result in a completely different hash, thereby alerting the network to potential tampering.
- **Block Addition**: Once a block is verified and accepted by the network, it is added to the blockchain. The new block then serves as the reference point for verifying the next block in the chain.

By employing hashing techniques and linking blocks through hashes, the block verification process ensures the immutability and security of data in a blockchain network.

D. Proxy re-encryption (PRE)

Schemes for proxy re-encryption (PRE) cryptographic systems that enable third-party proxies to modify a ciphertext originally encrypted for one party, making it decryptable by another. These schemes share similarities with traditional symmetric or asymmetric encryption, but introduce two additional functions:

Delegation: Using their secret key & the key of the designated user, the message recipient (keyholder) is given the ability to create a re-encryption key using this function. This re-encryption key is used by the proxy to convert ciphertexts to the key of the delegated user. Bi-directional or uni-directional asymmetric proxy re-encryption methods are both possible.

Transitivity: A ciphertext may be re-encrypted an infinite number of times using transitive proxy re-encryption methods. Non-transitive schemes, in contrast, only permit a specific amount of re-encryptions on an individual ciphertext. The majority of existing schemes are transitive and bidirectional.

The use of proxy re-encryption in online computing environments shows potential for safe sharing. In this instance, the cloud operator or administrator is given the re-encryption key. For instance, A creates a key for re-encryption for the internet to use if A wishes to share data to B via the cloud. However, difficulties can occur since a user might work with a cloud provider to acquire illicit access to a different user's files. The total amount of re-encryption keys increases proportionately with the amount of conditional values in segmentation via access control, creating problems for devices with limited resources. In Fig. 3, this procedure is depicted.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 10, October 2023 ||

| DOI:10.15680/IJIRSET.2023.1210032 |

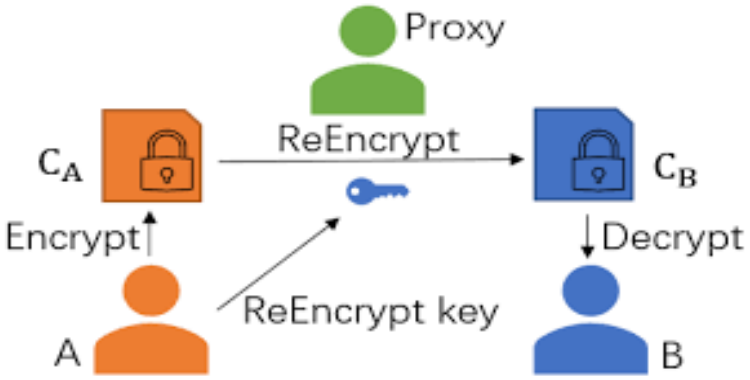

Fig 3: Proxy re-encryption

IV. PROPOSED WORK

The below Fig 4 shows a blockchain-based Employing a dynamic key generator, a proxy re-encryption mechanism is used to protect information exchanged in that Internet of Things (IoT). Its components include IoT devices responsible for generating and encrypting IoT data with dynamically generated keys. The Data Owner (DO) stores the dynamic key generator on the blockchain and issues registration keys to Data Users (DUs). DUs, in turn, store these keys on the blockchain and employ them to request IoT data from the DO. IoT data is encrypted and stored by a cloud service provider (CSP) and forwards DU requests to the proxy server. This server, acting as an edge node, executes proxy re-encryption using the DO's registration key and transmits the re-encrypted data to the DU. The blockchain, acting as a Trust Authority (TA), manages registration keys, the dynamic key generator, and re-encryption logs. The dynamic key generator plays a crucial role in generating time-limited keys for IoT devices and DUs, bolstering security against key compromise. This system architecture boasts enhanced security, scalability through blockchain integration, and auditability, presenting a promising advancement in IoT data security.

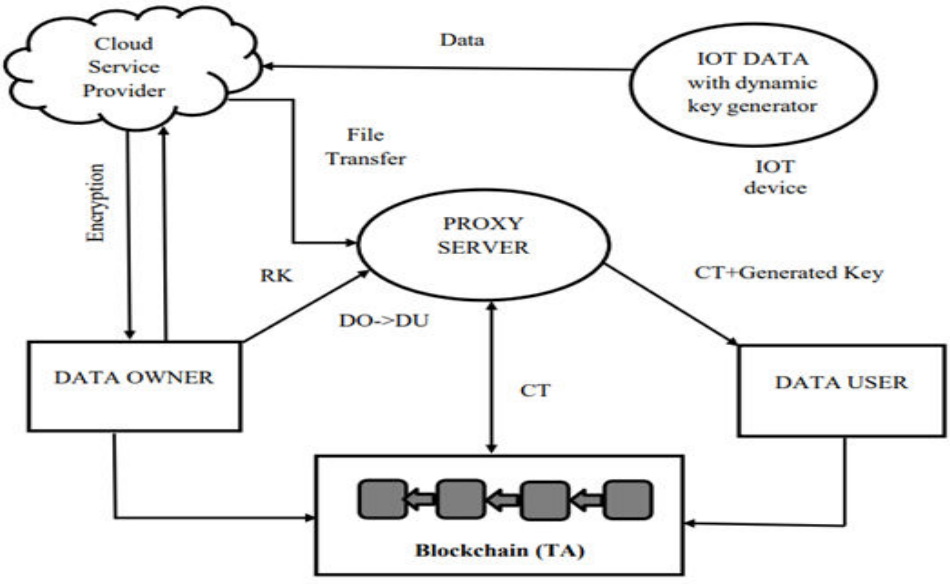

Fig 4: System Architecture

The suggested system uses a dynamic key generator and a blockchain-based proxy encryption mechanism to strengthen data exchange in the Internet of Things (IoT). This innovative architecture is designed to address key security concerns in IoT data sharing.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 10, October 2023 ||

| DOI:10.15680/IJIRSET.2023.1210032 |

1. User Verification: Within this system, users are required to verify their identities before gaining access to shared data. This robust authentication process serves as a critical barrier against unauthorized entry.

2. Data Ciphering: Before sharing data with authorized users, the system encrypts it using a robust encryption technique. This ensures that the confidentiality of shared data is maintained throughout the sharing process.

3. Dynamic Key Generation: The system employs a dynamic key generator that plays a pivotal role in generating time-limited keys for both IoT devices and Data Users (DUs). This adds an extra layer of security, significantly reducing the risk of key compromise.

4. Proxy Re-Encryption: One essential element of this approach is proxy re-encryption enabling secure data sharing without exposing the original data. This process is designed to be efficient while upholding the privacy of the shared data.

5. Access Management: The system leverages smart contracts to enforce access control policies, ensuring the integrity of shared data. These contracts efficiently enforce fine-grained access control policies, preventing unauthorized alterations to the shared data.

6. Blockchain Fusion: The integration with a blockchain is a key feature, guaranteeing the immutability and transparency of shared data. This blockchain securely and decentralistically stores the encrypted data and access control policies, adding an extra layer of security to the system.

7. Scalability: The system is engineered to efficiently handle a substantial number of devices and users, ensuring scalability without compromising security or efficiency.

8. User Interface: To enhance user experience, the system features an intuitive user interface. This empowers users to easily access shared data and perform operations like data sharing, key generation, and access control policy management.

This comprehensive system architecture not only addresses critical security concerns but also ensures scalability and ease of use. By integrating blockchain technology and dynamic key generation, it represents a significant advancement in IoT data security.

V. RESULT & DISCUSSION

The data in Table 1 illustrates the time required for uploading and downloading files of varying sizes, ranging from 1 MB to 15 MB. As the file size increases, both upload and download times tend to exhibit an upward trend. This observation is expected due to the increased computational overhead associated with larger files.Furthermore, it is evident that the download times are generally slightly shorter than upload times for the same file size. The data demonstrates the real-world applicability and efficiency of your blockchain-based proxy re-encryption method with dynamic key generation in securing data sharing within the IoT ecosystem. It highlights the trade-off between security and performance, providing valuable insights for optimizing system parameters and resource allocation to achieve the desired balance in practical IoT environments. These findings underscore the viability and effectiveness of your proposed solution for secure data sharing in IoT applications. Fig 5 shows the comparison time between uploading and downloading process.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 10, October 2023 ||

| DOI:10.15680/IJIRSET.2023.1210032 |

File size (MB)	Uploading	Downloading
1	180	130
2	280	154
3	420	174
4	640	222
5	600	250
6	1200	344
7	1260	510
8	1360	692
9	1440	870
10	1550	850
11	1700	1031
12	1850	1180
13	1920	1351
14	2140	1378
15	2300	1405

Table 1: Uploading & Downloading Time

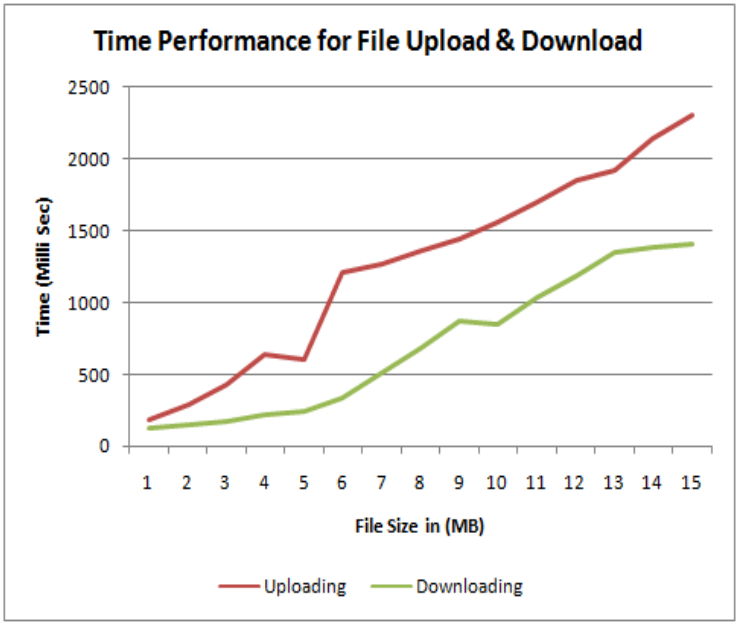

Fig 5: Time Comparison Graph

VI. CONCLUSION AND FUTURE WORK

Blockchain technology integration, Proxy Re-Encryption, and dynamic key generation signifies a transformative leap in securing IoT data. This framework acts as a potent defense against the escalating threat of data breaches and privacy violations accompanying the surge in IoT devices. The careful orchestration of these cutting-edge elements ensures not only robust data security but also enables seamless and confidential sharing across networks. Implementing blockchain as a distributed ledger fortifies the foundation, rendering it resistant to unauthorized access and tampering, instilling trust and accountability in the IoT ecosystem. Proxy Re-Encryption plays a crucial role, extending decryption capabilities without exposing sensitive cryptographic keys, striking a delicate balance between accessibility and security. The dynamic key generator introduces adaptability, autonomously responding to contextual cues and evolving conditions, future-proofing data protection. Empirical validation demonstrates the framework's effectiveness, excelling in safeguarding data integrity, scalability, and computational efficiency. Comparative assessments highlight the superiority and adaptability of the blockchain-based Proxy Re-Encryption approach. This methodology not only addresses privacy and confidentiality concerns but also sets the stage for a new IoT data management paradigm. By merging blockchain and dynamic key generation, this framework establishes a sturdy foundation for secure, scalable, and transformative IoT ecosystems, poised to revolutionize fields from healthcare to smart cities and industrial automation.

The path forward is illuminated, promising a future where IoT data exchange is characterized by unparalleled security and trust. To advance this research, key areas need exploration. Implement dynamic policy management for real-time access control adaptation. Optimize scalability for large-scale IoT networks to maintain efficiency. Develop efficient key management for resource-limited devices. Extend cross-domain data sharing. Integrate advanced security protocols like homomorphic encryption. Incorporate machine learning for anomaly detection. Refine the interface through usability studies. Ensure legal compliance and conduct real-world testing for practical applicability. These avenues strengthen the proposed IoT data sharing framework.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 10, October 2023 ||

| DOI:10.15680/IJIRSET.2023.1210032 |

REFERENCES

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.
[2] N. Park, "Secure data access control scheme using type-based reencryption in cloud environment," in Semantic Methods Knowledge Management and Communications. Berlin, Germany: Springer, 2011, pp. 319– 327.
[3] G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," Comput. Secur., vol. 30, no. 5, pp. 320–331, Jul. 2011.
[4] P. K. Tysowski and M. A. Hasan, "Hybrid attribute-and re-encryptionbased key management for secure and scalable mobile applications in clouds," IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172–186, Nov. 2013.
[5] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Inform. Sci., vol. 258, pp. 355–370, Feb. 2014.
[6] J. Han, W. Susilo, and Y. Mu, "Identity-based data storage in cloud computing," Future Gener. Comput. Syst., vol. 29, no. 3, pp. 673–681, Mar. 2013.
[7] H.-Y. Lin, J. Kubiatowicz, and W.-G. Tzeng, "A secure fine-grained access control mechanism for networked storage systems," in Proc. IEEE 6th Int. Conf. Softw. Secur. Rel., Jun. 2012, pp. 225–234.
[8] Y. Zhou et al., "Identity-based proxy re-encryption version 2: Making mobile access easy in cloud," Future Gener. Comput. Syst., vol. 62, pp. 128–139, Sep. 2016.
[9] X. A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure e-health cloud system using identity based cryptographic techniques," Future Gener. Comput. Syst., vol. 67, pp. 242–254, Feb. 2017.
[10] J. Shao, G. Wei, Y. Ling, and M. Xie, "Identity-based conditional proxy re-encryption," in Proc. IEEE Int. Conf. Commun., Jun. 2011, pp. 1–5.
[11] K. O. B. Obour Agyekum et al., "A secured proxy-based data sharing module in IoT environments using blockchain," Sensors, vol. 19, no. 5, Jan. 2019, Art. no. 1235.
[12] G. Zyskind et al., "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Secur. Privacy Workshops, May 2015, pp. 180–184.
[13] D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in Proc. IFIP Int. Conf. Distributed Appl. Interoperable Syst., Springer, Jun. 2017, pp. 206–220.
[14] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," IET Commun., vol. 12, no. 5, pp. 527–532, Mar. 2018.
[15] M. Singh and S. Kim, "Branch based blockchain technology in intelligent vehicle," Comput. Netw., vol. 145, pp. 219–231, Nov. 2018.
[16] R. S. Da Silva and S. D. Zorzo, "An access control mechanism to ensure privacy in named data networking using attribute-based encryption with immediate revocation of privileges," in Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf., Jan. 2015, pp. 128–133.
[17] B. Li, D. Huang, Z. Wang, and Y. Zhu, "Attribute-based access control for ICN naming scheme," IEEE Trans. Dependable Secure Comput., vol. 15, no. 2, pp. 194–206, Apr. 2016

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details