WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Integrating Blockchain and Proxy Re-encryption for Secure and Scalable IoT Data Sharing

Rutuja Killedar[a], Anand Kante[b], Sakshi Gawade[c], Swarupa Patil[d], Prof. Harshada M. Raghuwanshi[e], Prof. Vikramsingh R. Parihar[f]

[a,b,c,d]UG Students, Department of Computer Engineering, Trinity College of Engineering and Research, Pune.
[e]Assistant Professor, Department of Computer Engineering, Trinity College of Engineering and Research, Pune.
[f]Assistant Professor, Department of Electrical Engineering, Prof Ram Meghe College of Engineering & Management, Amravati.

A B S T R A C T :

This paper introduces a novel approach to enhancing data security in the IoT by combining blockchain technology with proxy re-encryption (PRE). The proposed framework uses blockchain for managing cryptographic keys and access control through smart contracts, while PRE facilitates secure, fine-grained data sharing among IoT devices without requiring intermediaries to decrypt the data. The paper details the system architecture, implementation, and evaluates its performance, showing that it effectively addresses security challenges like unauthorized access and data tampering, all while maintaining efficiency and scalability. This approach represents a major advancement in securing data in IoT environments.

Keywords: Blockchain , IoT, Data Security , Data Sharing , Re-encryption , cryptographic technique

1. Introduction

The Internet of Things (IoT) has transformed numerous industries by linking a vast array of devices, leading to new heights of automation and data sharing. This accumulation of IoT devices generates vast streams of data that can provide valuable insights but also pose significant security and privacy risks. The inherently distributed and dynamic nature of IoT environments complicates traditional security approaches, which often struggle to manage data integrity, confidentiality, and access control effectively. A major challenge in securing IoT data lies in the need for robust encryption mechanisms that protect sensitive information while allowing permitted access.

Proxy re-encryption (PRE) is a cryptographic technique designed to address these issues by enabling a third party to convert encrypted data from one encryption key to other without having access to the unencrypted data This method facilitates secure data sharing between entities with different encryption keys, potentially streamlining access control and enhancing security. However, traditional PRE solutions face limitations in scalability and key management, particularly in extensive IoT networks where the number of devices and access policies can become exceedingly complex.

Our approach utilizes blockchain-powered smart contracts to manage encryption keys and enforce access control policies, guaranteeing that only permitted entities can path and re-encrypt data. This integration enhances data security and also improves scalability and efficiency by automating key management and access control through decentralized consensus mechanisms. We will show the detailed design of the proposed framework, describe its implementation, and assess its effectiveness in terms of security, scalability, and operational efficiency. Through experimental results and analysis, we aim to demonstrate that our approach effectively addresses common security vulnerabilities in IoT networks, such as unauthorized data retrieval and data tampering, while maintaining practical performance levels.

2. RELATED WORKS

2.1. Pre-Data Sharing: In a standard PKE scheme, data is encoded using a receiver's public key, and only the matching private key can decrypt it. This ensures that only an intended recipient can read the data. Proxy Re-Encryption (PRE): PRE extends this concept by introducing an additional layer involving a "proxy" entity. The proxy can re-encode data from one recipient's format to another without decrypting it first.It allows the encrypted data can be securely converted for access by a different party.

Key Generation in Proxy Re-Encryption (PRE) : Alice generates a re-encoding key (RK_A→B) that enables a proxy to re-encoded ciphertexts originally encrypted with Alice's public key (PK_A) into a format that Bob is able to decrypt public key (PK_A) into a format that Bob can decrypt with his public key (PK_B). This process facilitates secure and flexible data sharing by allowing intermediaries (proxies) to transform encrypted data without accessing the plaintext.

Re-encryption : In the Proxy Re-Encryption (PRE) substructure is a secure transformation process performed by a proxy, which converts ciphertexts encrypted with one public key into ciphertext public key (PK_A) into a format that can be decrypted . This process maintains data confidentiality and allows flexible and secure data sharing between different parties.

Illustrative Example

Let's walk through a simple example to clarify:

- Alice wants to share a document securely with Bob.
  - She encrypts the document using her public key (PK_A), resulting in ciphertext CAC_ACA.
- Alice then generates a re-encoding key (RK_A→B) specifically for Bob.
  - She provides this re-encoding key to the proxy.
- The proxy receives CAC_ACA and RK_A→B.
  - Using RK_A→B, the proxy re-encoding CAC_ACA into CBC_BCB, which can be decrypted with Bob's public key (PK_B).
- Bob receives CBC_BCB.
  - Bob uses his personal key (SK_B) to decrypt CBC_BCB and access the original

Benefits of Proxy Re-Encryption

- Enhanced Security:
  - The proxy can convert ciphertexts without learning the plaintext data. This minimizes the risk of data exposure to intermediaries.
- Flexible Data Sharing:
  - PRE allows for secure data sharing without requiring the data owner to be involved in the decryption and re-encode process. This flexibility is crucial for dynamic access control and collaborative environments.
- Access Control Management:
  - The data owner can grant and revoke access by issuing or invalidating re-encryption keys, without needing to re-encrypt the data themselves or share it directly with the new recipients.

2.2 . Blockchain-Enabled Access Control And Data Sharing:

Blockchain-Enabled Access Control and data sharing represent a significant evolution in how digital resources are managed and protected.

1. Decentralization : Decentralization in blockchain-enabled access control enhances defense, transparency, and efficiency by distributing control across nodes. While it offers significant advantages over traditional centralized systems, it also introduces dare that must be tackled through scalable solutions, privacy considerations, and regulatory compliance. As blockchain technology evolves, its application in access control systems is likely to become more widespread and sophisticated.

2. Immutability: Immutability in blockchain-enabled access control and data sharing offers substantial benefits, including enhanced data integrity, defense, transparency, and compliance. It creates a reliable and trustworthy system for managing access and sharing information.

3. Transparency and testability: Transparency and testability in blockchain-enabled access control and data sharing provide substantial benefits, including enhanced security, trust, and compliance. Blockchain technology provides a distinct, immutable, comprehensive record of all transactions and changes, supporting effective monitoring and auditing.

4. Smart Contracts: Smart contracts significantly enhance blockchain-enabled access control and information exchange by automating processes, improving security, and ensuring transparency. They provide efficient and reliable mechanisms for managing authorization and executing data-sharing agreements, backed by the immutable nature of blockchain.

2.3 Blockchain-Enabled Data Sharing

1. Data Sovereignty: Data sovereignty in blockchain-enabled data sharing presents both opportunities and challenges. While blockchain technology offers transparency, security, and immutability, its global and decentralized nature can complicate compliance with local data protection laws. By leveraging hybrid blockchains, data localization strategies, encryption, and smart contracts, institutions can address these obstacles and guarantee that their data-sharing protocols align with data sovereignty requirements. Ongoing adaptation to regulatory changes and the creation of industry standards will further enhance the capability to efficiently handle data sovereignty in blockchain environments.

2. Security and Privacy: Blockchain technology offers significant benefits for data sharing in terms of security and privacy, including robust encryption, decentralized control, and immutable records. However, it also presents challenges such as balancing transparency with privacy, while adhering to data protection regulations, and addressing scalability issues. By leveraging advanced cryptographic techniques, privacy-enhancing technologies, and hybrid blockchain models, organizations can improve the security and privacy of blockchain-based data sharing systems while addressing the associated challenges.

3. Data Provenance: Blockchain-enabled data provenance provides significant benefits, including enhanced data integrity, transparency, accountability, and regulatory compliance. By leveraging blockchain's immutability and transparent record-keeping capabilities, organizations can effectively track the history and lineage of data, ensuring its authenticity and reliability. However, challenges such as data privacy, scalability, and implementation complexity must be resolved to fully unlock the potential of blockchain-based data provenance. Through careful planning, advanced cryptographic techniques, and hybrid solutions, organizations can harness the power of blockchain to improve data provenance and support trustworthy data sharing practices.

2.4 . Access Control Schemes for ICN :

Access control in Information-Centric Networking (ICN) is a key area of research and development due to the shift from host-centric networking to a model where data itself is the focal point. Unlike traditional IP networks, ICN emphasizes content rather than the location of content. This shift brings unique challenges and opportunities for access control.

1. Named Data Networking (NDN) Access Control : Access control in Named Data Networking (NDN) involves a combination of cryptographic techniques, policy frameworks, and efficient key management. While NDN's data-centric nature offers unique opportunities for securing and managing access to data, it also introduces challenges that need to be addressed to ensure secure and efficient data transport. Ongoing research and development are focused on refining these mechanisms and addressing the challenges associated with access control in NDN environments.

2. Content-Centric Networking (CCN) Access Control : Access control in Content-Centric Networking (CCN) involves a blend of cryptographic techniques, policy frameworks, and efficient key management. By focusing on data rather than hosts, CCN offers unique opportunities for secure and flexible access control. However, it also poses challenges that need to be tackled to ensure that access control mechanisms are both effective and scalable. Ongoing research and development are focused on refining these mechanisms to enhance security and performance in content-centric networks.

3. Key Management : Effective key management and distribution are fundamental for securing data in networks like NDN and CCN. By addressing challenges related to scalability, performance, security, and interoperability, robust key management practices can aid in ensuring the confidentiality, integrity, and authenticity of data throughout its lifecycle. As these networking paradigms evolve, ongoing advancements in cryptographic techniques and key management strategies will remain a crucial role in maintaining secure and efficient data-centric communications.

4. Policy-Driven Access Control : Policy-Driven Access Control (PBAC) provides a flexible and powerful framework for managing access to resources based on predefined rules and conditions. In networking environments like NDN and CCN, PBAC help guarantee that access to data is controlled and enforced according to specific policies. Implementing PBAC involves defining clear policies, managing their enforcement, and tackling issues associated with scalability, performance, privacy, and interoperability. As data-centric networks evolve, PBAC will continue to play a function in safeguarding and controlling access to data.

5. Authentication and Authorization : *Data Authentication: CCN provides built-in mechanisms for data authentication through digital signatures. Each data packet includes a signature that ensures data integrity and authenticity.*

Mutual Authentication: While CCN supports data authentication, mutual authentication (between users and data providers) often requires additional mechanisms. Protocols may be needed to authenticate users and verify that they have the right to access specific data.

6 . Encrypted Data Delivery : Complete encryption: CCN can support complete encryption, where data is encrypted before transmission and decrypted only by authorized recipients. Encryption can be combined with access control policies to ensure secure data delivery. Dynamic Key Exchange: Key management mechanisms in CCN can allow for dynamic key exchanges between data producers and consumers, providing controlled access to encrypted data.

7. Access Control Challenges : *Scalability: Managing access control in a scalable manner is crucial, particularly as the number of data items and users grows. Efficient key management and policy enforcement are essential for scalability.*

3. PROBLEM DEFINITION AND SYSTEM OVERVIEW

A. Problem Definition

Information exchange in the Internet of Things (IoT) has become widespread across various applications, including healthcare ,vehicular networks, smart residences, and energy transactions. Typically, when an IoT device—such as a sensor, pager, or smartphone -- wants to exchange its data with other users, the data is encrypted and sent to cloud storage.

Data owners are assumed to interact with other entities via a trusted intermediary or server that operates on a secure computer. The data user field includes legitimate recipients of the shared information, which can be both individuals and devices. These users must retrieve the shared data from the CSP, which, though semi-trusted, provides storage services without being privy to the plaintext of the information. The data is secured during transmission and can only be unsecured by authorized users. Despite its semi-trusted status, the CSP might have reasons to attempt to access the data.

To enhance service quality and optimize bandwidth usage, there are situations where a second user (user2) might need access todata previously exchanged between the data holder and a first user (user1).

B. System Model

Our proposed system framework, illustrated in Figure 2, integrates a blockchain-enabled Proxy Re-Encryption (PRE) advance towards optimizing data sharing. This model introduces two key entities—edge devices and the blockchain network—into the traditional data-sharing framework discussed in

Figure 1.

Edge bias These act as deputy bumps within the network, offeringre-encryption services to authorized users. deposited at the network edge, these bias cache data to enhance vacuity and performance. Edge bias admitere-encryption keys from data possessors, recoup ciphertext from the Cloud Service Provider(CSP), andre-encrypt the data for the specific stoner's identity. They're designed as honest- but-curious realities, icing they perform their functions rightly but may explore data for particular gain.

Acting as the Trusted Authority (TA), the blockchain sets up system parameters and issues secret keys linked to user identities. This distributed ledger ensures authenticity, transparency, and verifiability across the network, thereby enhancing data security and privacy. The blockchain records and distributes classification keys to both data owners and users. Data access requests are processed through the blockchain, which verifies users and enforces access rights.

Data Caching and Delivery

Our model incorporates data caching to improve content delivery resilience against packet losses, thereby enhancing content availability. This approach supports not only content caching, however, also functionality stashing, specifically re-encoding. Additionally, the multipoint delivery system of Information-Centric Networking (ICN) optimizes bandwidth and storage utilization. Asas the number of users grows, content is delivered through multiple points rather than anycast, thereby reducing overall bandwidth usage.

4. SYSTEM IMPLEMENTATION

In this section, we supply a detailed overview of the system workflow, including the functionality of the blockchain and the specifics of the re-encoding scheme.

4.1. System Workflow

The system workflow outlines how data is managed and accessed within our proposed framework. The process involves several key stages, each contributing to the overall data-sharing mechanism:

- **Initialization:** The Trusted Authority (TA) initializes the system by generating the necessary parameters and master secret key using the Setup algorithm. Concurrently, user keys are created using the KeyGen algorithm.
- **Data Encryption and Storage:** Data owners encrypt their data using the Encrypt algorithm, producing ciphertext (CT). This ciphertext is then outsourced to the Cloud Service Provider (CSP) for storage. Metadata, including access control policies and relevant cryptographic information, is recorded on the blockchain.
- **Data Access Request:** When a user requests access to data, the system verifies the user's identity through the blockchain. The data owner generates a re-encryption key specific to the user and sends it to the proxy server. Access rights and policies are enforced based on the blockchain's records.
- **Re-encryption and Data Retrieval:** The proxy server, acting as an intermediary, retrieves the ciphertext from the CSP using the provided re-encryption key. It then performs re-encryption, transforming the ciphertext for the requesting user. The re-encrypted data is sent to the user, who decrypts it using their private key.
- **Blockchain Verification:** Throughout the process, the blockchain ensures transparency and authenticity. Metadata, access control policies, and cryptographic proofs are recorded and verified on the blockchain, enabling secure and auditable data management.

Blockchain Functionality

The blockchain serves as the backbone of the system, providing a decentralized and tamper-resistant ledger. Its roles include:

- **Parameter Initialization:** The blockchain records the system parameters and master secret key generated during initialization. This ensures that all parties have access to the same foundational data.
- **Access Control Management:** The blockchain manages and verifies access control policies.It records and provides membership keys to both data holders and users, ensuring consistent enforcement of access rights
- **Auditing and Transparency:** All interactions related to data access requests, re-encryption, and metadata updates are logged on the blockchain.This ensures a clear and auditable trail of activities, enhancing the system's overall security.

4.2 Security Proof and Analysis

This section presents the security proof and analysis of our proposed cryptographic scheme. We also discuss the types of attacks our system is designed to counter.

1. Security Proof

To establish the security of our scheme, we employ formal security definitions and prove that our scheme meets these definitions under standard cryptographic assumptions. We focus on the following security aspects:

- **Semantic Security (IND-CPA):**We establish that the encryption scheme is robust against chosen-plaintext attacks (CPA). This indicates that an adversary with access to the encrypted data is unable to effectively extract any information regarding the plaintext without possessing the decryption key.

- **Unidirectionality of Re-encryption:** We demonstrate that the re-encryption process is inherently unidirectional. In particular, re-encryption keys facilitate the transformation of ciphertexts from the data owner to the data user, while preventing any reverse transformation. This guarantees that once data has been re-encrypted for a user, it cannot be reverted to the original format of the data owner.

Formal Proof of IND-CPA Security:

- **Security Model:**
  - Let A\mathematical{A}A be a competitor with access to encryption oracles and the ability to choose plaintexts.
  - The adversary is given a challenge ciphertext and needs to distinguish between two possible plaintexts.
- **Proof Outline:**
  - We demonstrate that if there is an efficient adversary A\mathcal{A}A capable of compromising the IND-CPA security of our scheme with a non-negligible probability, then it follows that there exists an efficient algorithm that can resolve a challenging problem within the bilinear map framework, such as the Decision Bilinear Diffie-Hellman (DBDH) problem.
  - We develop a reduction algorithm that leverages the adversary's success to address the DBDH problem, thereby illustrating that our scheme maintains a level of security equivalent to that of the foundational hard problem.

Formal Proof of Unidirectionality:

- **Security Model:**
  - We define unidirectionality as the property that the key renewal RKIDDO→IDDURK_{ID_{DO} \to ID_{DU}}RKIDDO →IDDU allows renewal encryption from the data programer ciphertext to the data user's ciphertext, but the process cannot be reversed.
- **Proof Outline:**
  - We illustrate that, utilizing a key renewal RKIDDO→IDDURK_{ID_{DO} \to ID_{DU}}RKIDDO→IDDU along with a ciphertext encrypted for the data owner, an adversary cannot acquire a key renewal that would allow the ciphertext to be transformed back to the original format of the data owner. The security of this mechanism relies on the difficulty of solving the underlying bilinear map problem.
  - This is founded on the premise that the key renewal includes the inverse of the decryption key, which does not permit reverse modification" due to the nature of the bilinear map and the hash functions used.

4.3. Attack Analysis

Our system is designed to withstand several types of attacks, including:

- **Chosen-Plaintext Attack (CPA):** Our scheme is proven to be CPA-secure, meaning that an adversary cannot gain any meaningful information about the plaintext from the ciphertext, even if they can choose plaintexts and observe their corresponding ciphertexts.
- **Chosen-Ciphertext Attack (CCA):** Although the primary security proof focuses on CPA, the scheme's design inherently resists CCA attacks due to the use of secure encryption and re-encryption techniques. However, a formal CCA proof may require additional steps or assumptions.
- **Replay Attacks:** The use of fresh random numbers rrr in encryption ensures that identical plaintexts produce different ciphertexts each time they are encrypted. This prevents adversaries from reusing old ciphertexts to infer information about new plaintexts.
- **Key Recovery Attacks:** The scheme's protect the obstacle of solving the underlying bilinear map Challenge (such as DBDH problem). Since recovering the decryption key or re-encryption key requires solving this hard problem, key recovery attacks are thwarted.
- **Unidirectionality Exploits:** The scheme's unidirectionality ensures that re-encryption keys cannot be used to revert the ciphertext to its original owner's format, thus preventing potential misuse of re-encryption keys.

5. PERFORMANCE EVALUATION

This section presents a comprehensive evaluation of the effectiveness of our proposed scheme. The assessment is divided into two main categories: functional comparison and performance analysis.

We assess the effectiveness of our proposed scheme based on various criteria and compare it with the schemes outlined:

- **Efficiency of Re-encryption:**
  - Our scheme provides efficient re-encryption operations due to its reliance on well-established bilinear map techniques. We compare the time complexity and computational overhead of re-encryption with those of the scheme
  - The scheme utilizes a hybrid approach, which may introduce additional computational overhead compared to a single technique. In contrast, our scheme leverages a more streamlined approach with potentially lower overhead.
- **Security and Practicality:**
  - We assess the security of our approach based on its resilience against known attacks and its robustness in various threat models. Our security proof is compared with the proofs provided.
  - Practical considerations such as ease of implementation and integration with existing systems are also assessed. Our scheme aims to balance security with practical deployment requirements.
- **Cost-Effectiveness:**
  - We analyze the cost implications of deploying our scheme compared to the other approaches. This includes computational costs, storage requirements, and any additional infrastructure needed.

- The scheme specifically emphasizes cost-effectiveness, making it a key reference for evaluating the cost-benefit ratio of our approach.

6. CONCLUSION

The rise of the machine-to-machine keeps highlighted data transfer as a key application. To ensure a secure method to maintain information security,data accuracy. Our approach uses the IBPRE technique to allow data owners to securely store encrypted data in the cloud and efficiently share it with authorized users. Due to resource constraints, an edge device serves as a proxy to manage the intensive computational tasks. Additionally, our program integrates Information-Centric Networking (ICN) features to upgrade content delivery by effectively utilizing network bandwidth and improving service excellence. We also introduce a cryptographic chain architecture that supports versatile access management for encoded data, enabling precise access control. This model helps data owners maintain privacy effectively. Our examination and findings illustrate the efficacy of the suggested model in accomplishing these objectives.

REFERENCES :

[1] Data Sharing," in *Proc. IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 99–103.

[2] Y. Zhang and S. Yu, "A Secure Data Sharing Scheme in Blockchain-Based IoT Using Proxy Re-Encryption," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 5211–5223, 2021.

[3] X. Chen, J. Zhang, Z. Huang, and Y. Xiang, "A Secure Data Sharing Framework for IoT Based on Blockchain and Proxy Re-Encryption," *J. Netw. Comput. Appl.*, vol. 168, 2020, Art. no. 102781.

[4] K. Zhao, P. Jiang, T. Xu, and C. Chen, "Secure Data Sharing in Blockchain-Based IoT Networks Using Proxy Re-Encryption and Attribute-Based Encryption," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7430–7441, 2020.

[5] J. Xu, Z. Zheng, J. Zhang, and Y. Liu, "Secure Data Sharing Scheme in Blockchain-Based IoT Systems Using Proxy Re-Encryption," *IEEE Access*, vol. 7, pp. 99732–99743, 2019.

[6] H. Hu, Y. Zhu, Y. Xu, and G. J. Ahn, "Secure and Efficient Data Sharing in Blockchain-Based IoT Systems Using Proxy Re-Encryption," *IEEE Trans. Ind. Inform.*, vol. 16, no. 2, pp. 1293–1302, 2020.

[7] H. Lee, S. Kim, and J. Park, "Blockchain-Assisted Attribute-Based Proxy Re-Encryption for Secure and Auditable IoT Data Sharing," *IEEE Trans. Ind. Inform.*, vol. 17, no. 4, pp. 2965–2973, 2021.

[8] Y. Zhang, X. Chen, X. Huang, J. Li, and H. Wang, "Blockchain-Based Data Sharing for IoT Devices Using Proxy Re-Encryption," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9076–9084, 2019.

[9] D. He, H. Luo, H. Huang, "Secure Data Sharing in Blockchain-Based IoT Networks Using Proxy Re-Encryption and Dynamic Key Management," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 5946–5956, 2019.

[10] Y. Sun, L. Xu, and L. Zhang, "Secure Data Sharing in Blockchain-Based IoT Systems Using Proxy Re-Encryption and Shamir's Secret Sharing," IEEE Access, vol. 8, pp. 155527–155536, 2020.

[11] D. Huang and C. Xie, "Secure Data Sharing in Blockchain-Based IoT Using Proxy Re-Encryption and Access Control," Proc. IEEE Int. Conf. Internet of Things (iThings), pp. 1701–1706, 2020.

[12] Y. Zeng, H. Xiong, J. Xu, and H. Zhang, "A Secure Data Sharing Scheme in Blockchain-Based IoT Using Proxy Re-Encryption and Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Int. Conf. Communications Workshops (ICC Workshops), pp. 1–6, 2020.

[13] J. Cao, C. Wu, and Y. Yang, "A Secure Data Sharing Scheme in Blockchain-Based IoT Systems Using Proxy Re-Encryption and Elliptic Curve Cryptography," Proc. Int. Conf. Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 83–88, 2019.

[14] Q. Liu, Y. Zhang, and X. Zheng, "A Secure Data Sharing Scheme in Blockchain-Based IoT Using Proxy Re-Encryption and Chaotic Map," Proc. Int. Conf. Computer Science and Cloud Computing (CSCC), pp. 74–80, 2021.

[15] Vikramsingh R. Parihar, Graph Theory Based Approach for Image Segmentation Using Wavelet Transform, International Journal of Image Processing (IJIP), Volume 8, Issue 5, pp 255-277, Sept 2014

[16] Vikramsingh R. Parihar, Heartbeat and Temperature Monitoring System for Remote Patients using Arduino, International Journal of Advanced Engineering Research and Science (IJAERS), Volume 4, Issue 5, PP 55-58, May 2017

[17] Vikramsingh R. Parihar, PC Controlled Electrical Line Cutting System, International Journal of Engineering Science and Computing (IJESC), Volume 7, Issue 5, pp 11380-11381, May 2017

[18] Vikramsingh R. Parihar, Overview and an Approach to Develop a Four Quadrant Control System for DC Motors without using Microcontroller, International Journal of Engineering Science and Computing (IJESC), Volume 7, Issue 5, pp 11879-11881, May 2017

[19] Vikramsingh R. Parihar, Image Analysis and Image Mining Techniques: A Review, Journal of Image Processing and Artificial Intelligence (MAT Journals), June 2017

[20] Vikramsingh R. Parihar, Power Transformer Protection using Fuzzy Logic based Controller, International Journal of Engineering Research (IJER), Volume 6, Issue 7, pp 366-370, July 2017

[21] Vikramsingh R. Parihar, Overview and an Approach to Real Time Face Detection and Recognition, International Advanced Research Journal in Science, Engineering and Technology (IARJSET), Volume 4, Issue 9, PP 39-46, Sept 2017

[22] Vikramsingh R. Parihar, Neural Network and Fuzzy Logic Based Controller For Transformer Protection, International Journal of Current Engineering and Scientific Research (IJCESR), Volume 4, Issue 9, PP 33-38 , Sept 2017

[23] Vikramsingh R. Parihar, A Novel Approach to Power Transformer Fault Protection using Artificial Neural Network, International Journal of Current Engineering and Scientific Research (IJCESR), Volume 4, Issue 9, PP 33-38, Sept 2017

[24] Vikramsingh R. Parihar, Power Transformer Fault Protection using Artificial Neural Network, Journal of Electrical and Power System Engineering (MAT Journals), Volume 3, Issue 3, pp 1-5 , Sept 2017

[25] Vikramsingh R. Parihar, Fuzzy Logic based Controller for Power Transformer Protection, Journal of Electrical and Power System Engineering (MAT Journals), Volume 3, Issue 3, pp 1-5 , Oct 2017

[26] Vikramsingh R. Parihar, Real Time Face Detection and Recognition: Overview and Suggested Approach, Journal of Image Processing and Artificial Intelligence (MAT Journals), Volume 3, Issue 3, pp 1-6, Sept 2017
[27] Vikramsingh R. Parihar, A Novel Approach to Real Time Face Detection and Recognition, International Journal of Computer Sciences and Engineering (IJCSE), Volume 5, Issue 9, pp 62-67, Sept 2017
[28] Vikramsingh R. Parihar, Automatic Irrigation System Using Android Mobile: A Review, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Volume 6, Issue 9, pp 200-203, Oct 2017
[29] Vikramsingh R. Parihar, Transmission Line Multiple Fault Detection: A Review and an Approach, International Journal of Current Engineering and Scientific Research (IJCESR), Volume 4, Issue 10 pp 1-7, Oct 2017
[30] Vikramsingh R. Parihar, Regenerative Braking System for Energy Harvesting from Railways and Vehicles: A Review and an Approach, International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), Volume 5, Issue 10, pp 18-25, Oct 2017
[31] Vikramsingh R. Parihar, RFID Based Student Attendance Management System: A Review and an Approach, International Advanced Research Journal in Science, Engineering and Technology (IARJSET), Volume 4, Issue 9, pp 262-265, Sept 2017
[32] Vikramsingh R. Parihar, Distance Protection Problem in Series-Compensated Transmission Lines, International Journal of Advanced Trends in Technology, Management and Applied Science (IJATTMAS), Volume 3, Issue 10, pp 44-48, Oct 2017
[33] Vikramsingh R. Parihar, Series-Compensated Transmission Line Problem in Distance Protection, International Journal of Electrical, Electronics and Communication Engineering (IJEECE), Volume 3, Issue 10, pp 1-9, Oct 2017
[34] Vikramsingh R. Parihar, Series Compensated Line Protection using Artificial Neural Network, International Advanced Research Journal in Science, Engineering and Technology (IARJSET), Volume 4, Issue 10, pp 102-111, Oct 2017
[35] Vikramsingh R. Parihar, Protection Scheme of Fault Detection in High Voltage Transmission Line, International Journal of Advanced Trends in Technology, Management and Applied Science (IJATTMAS), Volume 3, Issue 11, pp 1-4, Nov 2017
[36] Vikramsingh R. Parihar, IOT Based Communication Technology for High Voltage Transmission System, Journal of Electrical and Power System Engineering (MAT Journals), Volume 3, Issue 3, pp 1-6 , Nov 2017
[37] Vikramsingh R. Parihar, Transmission Line Protection Analysis using STATCOM, International Journal of Advanced Trends in Technology, Management and Applied Science (IJATTMAS), Volume 3, Issue 11, pp 23-26, Nov 2017
[38] Vikramsingh R. Parihar, A Review on Transmission Line Fault Detection Techniques, International Journal of Advanced Trends in Technology, Management and Applied Science (IJATTMAS), Volume 3, Issue 11, pp 27-32, Nov 2017
[39] Vikramsingh R. Parihar, Transmission Line Protection using Distance Relays, International Journal of Electrical, Electronics and Communication Engineering (IJEECE), Volume 3, Issue 1, pp 1-15, Nov 2017
[40] Vikramsingh R. Parihar,Protection of Power Transformers using Artificial Neural Network and Fuzzy logic, International Journal of Advanced Trends in Technology, Management and Applied Science (IJATTMAS), Volume 3, Issue 11, pp 72-79, Nov 2017
[41] Vikramsingh R. Parihar, Control System Security: An Issue, Journal of Control System and Control Instrumentation (MAT Journals), Volume 3, Issue 3, pp 1-5 , Dec 2017
[42] Vikramsingh R. Parihar, Resilient Designs of Control Systems Analysis and Review, Journal of Control System and Control Instrumentation (MAT Journals), Volume 3, Issue 3, pp 1-9 , Dec 2017
[43] Vikramsingh R. Parihar,Industrial Control System Cyber Security: Review & Recommendations, Journal of Network Security Computer Networks (MAT Journals), Volume 3, Issue 3, pp 1-9 , Dec 2017
[44] Vikramsingh R. Parihar,Operational Analysis of Infrared Gas Sensor, Journal of Instrumentation and Innovation Sciences (MAT Journals), Volume 4, Issue 1, pp 1-5 , Dec 2017
[45] Vikramsingh R. Parihar, Automatic Fault Detection in Transmission Lines using GSM Technology, International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), Volume 6, Issue 4, pp 90-95, April 2018
[46] Vikramsingh R. Parihar, UPFC based distance relays for protection of transmission systems employing FACTS, International Journal of Advanced Engineering and Technology (IJAET), Volume 2, Issue 2, pp 4-7, May 2018
[47] Vikramsingh R. Parihar, Power Substation Protection from Lightening Over voltages and Power Surges, International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), Volume 6, Issue 6, pp 26-31, June 2018
[48] Vikramsingh R. Parihar, An Overview of Transmission Line Fault Detection Techniques, International Journal of Innovative Research & Studies (IJIRS), Volume 8, Issue VII, pp 64-77, July-2018
[49] Vikramsingh R. Parihar, Power Monitoring System Using Microcontroller for Optimum Power Utility in homes, Reinvention International: An International Journal of Thesis Projects and Dissertation, Volume 1, Issue 1, pp 96-112, Aug-2018
[50] Vikramsingh R. Parihar, Automatic Wireless Health Monitoring System, Reinvention International: An International Journal of Thesis Projects and Dissertation, Volume 1, Issue 1, pp 84-95, Aug-2019
[51] Vikramsingh R. Parihar, Overview and an Approach for QR-Code Based Messaging and File Sharing on Android Platform in View of Security, Proceedings of the IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC), July 2017
[52] Vikramsingh R. Parihar, Line Trap and Artificial Intelligence Based Double Circuit Transmission Line Fault Classification, International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS 2017), August 2017
[53] Vikramsingh R. Parihar, Hybrid Power System with Integration of Wind, Battery and Solar PV System, IEEE International Conference on Power, Control, System and Instrumentation Engineering (ICPCSI), Sept 2017
[54] Vikramsingh R. Parihar, A Novel System of Real Time Hand Tracking and Gesture Recognition, IEEE International Conference on Inventive Computing and Informatics (ICICI), Nov 2017.
[55] Vikramsingh R. Parihar, Improving Power Quality of Induction Motors using Capacitor Bank, International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), Volume 6, Issue 9, pp 37-45, Sept 2018
[56] Vikramsingh R. Parihar, Power Generation from Exhaust Gases of Diesel Engines: An Overview and an Approach, International Advanced Research Journal in Science, Engineering and Technology (IARJSET), Volume 5, Issue 9, pp 66-74, Sept 2018
[57] Vikramsingh R. Parihar, Power Quality Disturbance Eviction using SOM Neural Network, Journal of Recent Advances in Electronics and Communication Engineering, Volume 1, Issue 1, pp 1-15, Oct 2018
[58] Vikramsingh R. Parihar, Optimized Neural Network Based Classifier for Effective Classification of Power Quality Disturbances, Journal of Recent Advances in Electronics and Communication Engineering, Volume 1, Issue 1, pp 16-31, Oct 2018
[59] Vikramsingh R. Parihar, A Review and an Approach of Water Pollution Indication using Arduino Uno, International Journal of Advanced Engineering Research and Science (IJAERS), Volume 5, Issue 10, pp 160-167, Oct- 2018
[60] Vikramsingh R. Parihar, A Review and an Approach of Flying Electric Generators as Alternate Source of Energy, International Journal of Advanced Engineering Research and Science (IJAERS), Volume 5, Issue 10, pp 173-178, Oct- 2018
[61] Vikramsingh R. Parihar, Automatic Overhead Water Tank Cleaning System: A Review and an Approach, International Journal of Advanced Engineering Research and Science (IJAERS), Volume 5, Issue 10, pp 185-194, Oct- 2018
[62] Vikramsingh R. Parihar, Transmission Line Symmetrical Faults Protection System, Journal of Recent Advances in Electronics and Communication Engineering, Volume 1, Issue 1, pp 32-37, Oct 2018

[63] Vikramsingh Parihar, Hamid Reza Boveiri, "Research Directions and Future Trends in Medical Image Segmentation," ICSES Transactions on Image Processing and Pattern Recognition, vol. 5, no. 2, pp. 1-3, Jun. 2019.

[64] Vikramsingh R. Parihar, Two Way Wireless Mesh Network Data Sharing between ESP8266 without Internet, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Volume 8, Issue 8, pp 23-28, Aug 2019

[65] Vikramsingh Parihar, Hamid Reza Boveiri, Image Segmentation: A Guide to Image Mining. ICSES Transactions on Image Processing and Pattern Recognition (ITIPPR), ICSES, pp. 1-250, 2018. DOI: 10.31424/icses.itippr.2018.v4.n4

[66] Altaf Shah, Vikram Parihar, "An Easy Approach to JAVA: Let's code"

[67] Vikramsingh Parihar, Hamid Reza Boveiri, "A Survey and Comparative Analysis on Image Segmentation Techniques," in Image Segmentation: A Guide to Image Mining, 1st ed., ITIPPR: ICSES, 2018, pp. 1-15.

[68] Vikramsingh Parihar, Roshani Nage, Atul Dahane, "A Novel Graph-based Image Mining Technique Using Weighted Substructure," in Image Segmentation: A Guide to Image Mining, 1st ed., ITIPPR: ICSES, 2018, pp. 16-25.

[69] Vikramsingh Parihar, "Image Segmentation Based on Graph Theory and Threshold," in Image Segmentation: A Guide to Image Mining, 1st ed., ITIPPR: ICSES, 2018, pp. 61-82.

[70] Vikramsingh Parihar, Roshani Nage, Atul Dahane, "A Review and Comparative Analysis on Image Mining Techniques ," in Image Segmentation: A Guide to Image Mining, 1st ed., ITIPPR: ICSES, 2018, pp. 51-60.

[71] Ashish R. Varma, Surbhi S. Kashyap, Vikramsingh Parihar, "Challenges in Cloud Computing and Big Data, and their Solution using Hadoop", Innovation, Opportunities and Challenges in Big Data, Eureka Publications, pp 63-74, 2019, ISBN 978-81-938863-0-4

[72] Ashish R. Varma, Surbhi S. Kashyap, Vikramsingh Parihar, "Design and Implementation of

[73] Optimum Replica Management in HDFS", Innovation, Opportunities and Challenges in Big Data, Eureka Publications, pp 100-133, 2019, ISBN 978-81-938863-0-4

[74] Ashish R. Varma, Surbhi S. Kashyap, Vikramsingh Parihar, "Novel Approach for Providing High

[75] Storage Efficiency in HDFS", Innovation, Opportunities and Challenges in Big Data, Eureka Publications, pp 139-155, 2019, ISBN 978-81-938863-0-4

[76] Ashish R. Varma, Surbhi S. Kashyap, Vikramsingh Parihar, "Study of Different Approaches used In Heterogeneous Cluster to provide Higher Access and Consistency for Big Data", Innovation, Opportunities and Challenges in Big Data, Eureka Publications, pp 173-190, 2019, ISBN 978-81-938863-0-4

[77] Vikramsingh Parihar, Hamid Reza Boveiri, "A Survey and Comparative Analysis on Image Segmentation Techniques," in Image Segmentation: A Guide to Image Mining, 1st ed., ITIPPR: ICSES, 2018, pp. 1-15.

[78] Vikramsingh Parihar, Roshani Nage, Atul Dahane, "A Novel Graph-based Image Mining Technique Using Weighted Substructure," in Image Segmentation: A Guide to Image Mining, 1st ed., ITIPPR: ICSES, 2018, pp. 16-25.

[79] Vikramsingh Parihar, "Image Segmentation Based on Graph Theory and Threshold," in Image Segmentation: A Guide to Image Mining, 1st ed., ITIPPR: ICSES, 2018, pp. 61-82.

[80] Vikramsingh Parihar, Roshani Nage, Atul Dahane, "A Review and Comparative Analysis on Image Mining Techniques ," in Image Segmentation: A Guide to Image Mining, 1st ed., ITIPPR: ICSES, 2018, pp. 51-60.

[81] Vikramsingh R. Parihar, “Wireless Communication Technology using Li-Fi”, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 8, Issue 9, pp. 38-41. September 2019,

[82] Vikramsingh R. Parihar, Solar Power Tracking Device using Embedded Systems, International Journal of Creative Research Thoughts (IJCRT), Volume 9, Issue 7, pp f388-f401, July 2021

[83] Vikramsingh R. Parihar, Distance Calculation for Underground Cable Fault, International Journal of Creative Research Thoughts (IJCRT), Volume 9, Issue 7, pp f776-f796, July 2021

[84] Vikramsingh R. Parihar, Minimizing Penalty in Industrial Power Factor by Engaging APFC Unit, International Journal of Computer Science (IJCS), Volume 10, Issue 2, pp 2936-2947, Aug 2022

[85] Vikramsingh R. Parihar, AUTO SELECTION OF ANY AVAILABLE PHASE IN THREE PHASE SUPPLY SYSTEM, International Journal of Computer Science (IJCS), Volume 10, Issue 2, pp 2948-2960, Aug 2022

[86] Vikramsingh R. Parihar, Repercussions of Anti Satellite Missile Tests Alternate ASAT Technologies and Preventive Techniques for Mitigation of Space Debris, International Journal of Scientific Research in Engineering and Management (IJSREM), Volume 8, Issue 4, pp 1-8, April 2024

[87] Vikramsingh R. Parihar, Kidney Stone Prediction using Neural Network, Ajanta, Volume 13, Issue 2, April 2024

[88] Vikramsingh R. Parihar, Roshani S. Nage, Harshada M. Raghuwanshi, Mohini G. Fuse, Dr. Soni A. Chaturvedi, "Power Transformer Faults: Analysis, Classification and Protection," Engineering World, vol. 6, pp. 215-224, 2024, DOI:10.37394/232025.2024.6.23

[89] Vikramsingh R. Parihar, Rohan V. Thakur, Dr. Mohan B. Tasare, Harshada M. Raghuwanshi, Mohini G. Fuse, Dr. Soni A. Chaturvedi, "Inverter Coupled Energy Storage System for Soft-Restarting of Power System Dynamic Load," International Journal on Applied Physics and Engineering, vol. 3, pp. 52-58, 2024, DOI:10.37394/232030.2024.3.8

[90] Vikramsingh R. Parihar, Aaditya P. Agarkar, Kaustubh S. Kalkonde, Harshada M. Raghuwanshi, Mohini G. Fuse, Dr. Soni A. Chaturvedi, "Series Active Power Filter for Power Quality Improvement," Engineering World, vol. 6, pp. 234-239, 2024, DOI:10.37394/232025.2024.6.25

[91] Vikramsingh R. Parihar, Roshani S. Nage, Krunal S. Panpaliya, Yogesh P. Khadse, Kaustubh S. Kalkonde, Dr. Soni A. Chaturvedi, "Adaptive Approach for Power Oscillation Damping using STATCOM," Engineering World, vol. 6, pp. 225-233, 2024, DOI:10.37394/232025.2024.6.24

[92] Aaditya P. Agarkar, Vishalsing V. Bais, Chetan R. Ingole, Amol. P. Bhagat, Vikramsingh R. Parihar, "Automatic UPI based Medicine Vending Machine using IOT", First International Conference on Multidisciplinary Research 2024 (FICMR 2024)