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 11, Issue 8, August 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

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: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108133 |

# A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain

**Mr.A.JEEVA., [1] Mr.M.SATHISH.,[2]**

Assistant Professor, Department of Master of Computer Application, Gnanamani College of Technology,Namakkal Tamilnadu, India[1]

PG Scholar, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal, Tamilnadu, India[2]

**ABSTRACT:** A secure access control framework to realize data confidentiality and fine-grained access to data are achieved. This will also guarantee data owners' complete control over their data. Data owners can outsource their encrypted data to the cloud using identity-based encryption, while proxy re-encryption construction will grant legitimate users access to the data. With the Internet of Things devices being resource-constrained, an edge device acts as a proxy server to handle intensive computations. Also, we make use of the features of information-centric networking to deliver cached content in the proxy effectively, thus improving the quality of service and making good use of the network bandwidth. Further, our system model is based on block chain, a disruptive technology that enables decentralization in data sharing. This action proposes the concept of pre- authentication because the preceding time, i.e., only customers together with assured attributes that hold already. The pre-authentication mechanism combines the blessings over proxy subject re- encryption multi-sharing mechanism with the attribute- based authentication technique, as a consequence accomplishing attributes authentication earlier than re- encryption, then making sure the safety concerning the attributes yet data. Moreover, this action sooner or later proves to that amount the system is secure yet the proposed pre-authentication mechanism could appreciably enhance the law protection level.

**KEYWORDS***:* Attribute-based proxy re-encryption, Data sharing, Cloud computing, Verifiability.

## I. INTRODUCTION

The Internet of Things (IoT) has emerged as a technology that has great significance to the world nowadays and its utilization has given rise to an expanded growth in network traffic volumes over the years. It is expected that a lot of devices will get connected in the years ahead. Data is a central notion to the IoT paradigm as the data collected serves several purposes in applications such as healthcare, vehicular networks, smart cities, industries, and manufacturing, among others. The sensors measure a host of parameters that are very useful for stakeholders involved. Consequently, as enticing as IoT seems to be, its advancement has introduced new challenges to security and privacy. IoT needs to be secured against attacks that hinder it from providing the required services, in addition to those that pose threats to the confidentiality, integrity, and privacy of data. A viable solution is to encrypt the data before outsourcing to the cloud servers. Attackers can only see the data in its encrypted form when traditional security measures fail. In data sharing, any information must be encrypted from the source and only decrypted by authorized users in order to preserve its protection.

Conventional encryption techniques can be used, where the decryption key is shared among all the data users designated by the data owner. The use of symmetric encryption implies that the same key is shared between the data owner and users, or at least the participants agree on a key. This solution is very inefficient. Furthermore, the data owners do not know in advance who the intended data users are, and, therefore, the encrypted data needs to be decrypted and subsequently encrypted with a key known to both the data owner and the users. This decrypt-and-encrypt solution means the data owner has to be online all the time, which is practically not feasible. The problem becomes increasingly complex when there are multiple pieces of data and diverse data owners and users. Although simple, the traditional encryption schemes involve complex key management protocols and, hence, are not apt for data sharing. Proxy re-encryption (PRE), a notion first proposed by Blaze et al. , allows a proxy to transform a file computed under a delegator's public key into an encryption intended for a delegate. Let the data owner be the delegator and the data user

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108133 |

be the delegate. In such a scheme, the data owner can send encrypted messages to the user temporarily without revealing his secret key. The data owner or a trusted third party generates the re-encryption key. A proxy runs the re-encryption algorithm with the key and revamps the ciphertext before sending the new ciphertext to the user. This is the block chain technology, and it has gained much attention due to its ability to preserve data privacy. Although there exist optimization issues when storing vast sizes of data, emerging system applications have used the block chain for access control in database management. Data confidentiality and user revocation can also be achieved using block chain. PRE, together with IBE and the features of ICN and block chain, will enhance security and privacy in data-sharing systems. PRE and IBE will ensure fine-grained data access control, while the concept of ICN promises a sufficient quality of service in data delivery because the in-network caching provides efficient distribution of data. The block chain is optimized to prevent storage and data-sharing overheads and also to ensure a trusted system among entities on the network. In our article, the data owner propagates an access control list which is stored on the block chain. Further, our system model is based on block chain, a disruptive technology that enables decentralization in data sharing. It mitigates the bottlenecks in centralized systems and achieves fine-grained access control to data. The security analysis and evaluation of our scheme show the promise of our approach in ensuring data confidentiality, integrity, and security. Fine-grained access control is achieved, and it can help data owners achieve privacy preservation in an adequate way. The analysis and results of the proposed model show how efficient our scheme is, compared to existing schemes.

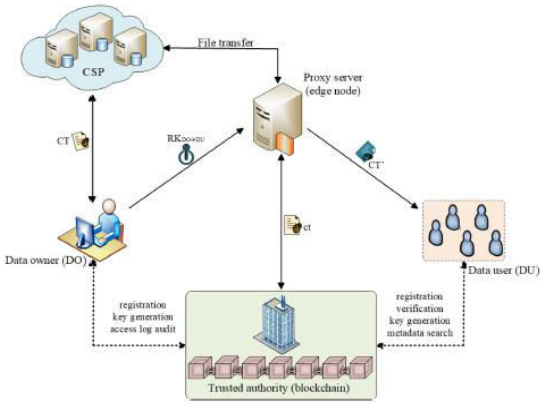


**Fig 1 System Architecture**

## II. LITERATURE REVIEW

With the rapid advancement of Internet of Things (IoT) technology, massive IoT devices have been deployed to different application scenarios. A fantastic amount of data is generated every day all over the world by these devices. Data are the core concept of IoT technology, and these data are of inestimable value in different applications. Although IoT seems to be very attractive, its advances have brought new challenges to security and privacy. Consequently, there is an imperative need to guarantee the reliability and security of IoT data sharing IoT data sharing has played a vital role in smart cities, healthcare, vehicular networks and other application fields depicts a popular data sharing architecture. The data producer domain contains a series of sensors and other devices that can collect data directly. The data owners generate and manage a large amount of IoT data. Due to the limited storage capacity of IoT devices, these massive data need to be encrypted and uploaded to a third party for storage, which is convenient for data management, distribution and sharing. They can encrypt the data and upload them to the storage service providers, such as cloud servers and distributed file systems for storage. The ownership of the data belongs to the data owner domain. In order to facilitate the sharing of data with other users, access rights are usually bound to the encrypted data itself and outsourced to storage service providers for management. Therefore, it is necessary to establish an effective access control mechanism to ensure the privacy and security of data owners, but this task is usually quite challenging. Data sharing depends on semi-trusted storage service providers, and they may have incentives for trying to read the data. At the same time, the process of authentication and revocation of data access rights is also opaque to the data owners. Since the data are encrypted, the users also lack an entirely credible communication channel to share the decryption

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108133 |

key. Moreover, the data sharing depends on storage service providers, which will bring excellent communication overload. If the data owners want to share data with the receivers directly, they need to download the data, decrypt and re-encrypt them for data sharing. This calculation and communication overload is enormous. However, the computing power of the data owners is limited, and they cannot afford to decrypt the encrypted data and then encrypt it to the receivers. Therefore, they can share IoT data with the help of the proxy re-encryption mechanism. In this way, the task of the data owners can be changed from the encryption and decryption process of ciphertext to the generation process of a re-encryption key, which distributes the overload on the data owners.

The Internet of things (IoT) refers to a network in which information from all connected devices can be collected, processed, and modified to provide new services. The IoT can be used in various ways, and the data transmitted during network communication can take many forms, ranging from personal data to sensing information gathered from the environment. If an attacker were to collect such data and use it maliciously, greater security threats would naturally arise in the IoT than in the existing environment. Passive attacks, such as spam messages sent via refrigerators or smart TVs, may result in damage to these devices, and more aggressive attacks may even threaten the user's life; for example, by hacking vehicle communication systems or medical devices. Furthermore, user data collected on IoT platforms can result in privacy invasion; for example, electricity consumption pattern analysis using a smart meter could expose a person's lifestyle. Although users can enjoy the benefits of data being collected to provide customized services, some may not wish to expose their personal data to service providers. Considering the factors mentioned above, data transmission security in the IoT environment is vital for managing multiple forms of personal data and avoiding damage caused by security threats.

Data sharing has become a very common practice amongst individuals, educational organizations, scientific communities, and medical industry. Industries and financial institutions have to heavily rely on data sharing within the organization as well as outside the organization. For example, banks need to share documents internally among the employees as well as externally with the account holders. Educational institutions share data with students, faculties and staffs. Scientific communities share data among themselves for collaboration and knowledge sharing purposes. Medical industry also shares data among patients, different healthcare professionals, pharmacies, and insurance payers for better interoperability. People are constantly sharing their photos, videos, life-events, stories, views, opinions, etc. in different social media platforms such as Facebook, Instagram, Youtube, Vine, TikTok, and Twitter to stay connected with each other regardless of their geographical distance. Moreover, with the recent wide adoption of IoT devices, knowingly or unknowingly people are sharing data everyday with IoT service providers. For example, smart wearable like apple watch and fit bit send activity data to the service provider's server to perform analytic on the data. Smart home assistant like Google home or Amazon Alexa continuously exchanges data with the respective service provider. Cloud and IoT service provider cannot be fully trusted with the sensitive user data because they are prone to insider and outsider attacks. For example, sensitive information (including date of birth and SSN) of nearly 143 million users was allegedly compromised11355 2 due to the Equifax data breach 1. Moreover, they can misuse data or sell it to third-party for financial benefit. Such unwanted incidents can be avoided and the benefits of cloud and IoT can be enjoyed to their full potential by designing secure data sharing schemes.

The rapid development of information diversification, cloud storage is becoming progressively popular in our daily life. Cloud storage allows businesses or individuals to access cloud data anytime, anywhere, and this feature provides incredible access to our lives. First, shared data must be encrypted to ensure data confidentiality. Second, the complexity of data security is increasing and the efficiency of data exchange is decreasing. Many cloud storage systems are also managed by a centralized company with powerful storage and monitoring, so the company must consider a third party to inherit any failure. am. Finally, it is important to update the cloud storage of the equipment, and with an increase in employee wages, the centralized cloud storage cost is rapidly increasing. Therefore, you must implement flexible access control through encrypted data to better ensure the confidentiality of data and data availability, and you must move data storage devices from a centralized system to a distributed system, not inexpensive than an existing centralized storage system. The Internet of Things provides tremendous convenience to people's daily lives by exchanging data and making full judgments. However, it creates security and privacy concerns. Block chain technology has the ability to overcome these privacy concerns in the IoT. In this article, they talk over the most prevalent privacy issues with the IoT. Then, in order to address these issues, block chain-based solutions are given a block chain based technology is being developed to address the issue of privacy leaks at the time of data sharing in the internet with the help of fine access control mechanism. To begin, this article introduces novel hierarchical attribute-based encryption technique that makes use of both a hierarchical and a multi-level authorization structure. By allocating separate user characteristics to distinct authorization centers, the approach enables fine-grained access control (FA). On a block chain, a smart contract performs partial decryption to minimize user decryption costs. Additionally, blockchain technology enables the tractability of earlier acts, which satisfies data security standards for restriction, openness, and

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108133 |

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

## III. METHODOLOGIES

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

### DATA SHARING BASED ON PROXY RE-ENCRYPTION MECHANISM

Much research work has been carried out around the data-sharing scheme based on the proxy re-encryption mechanism. Attendee proposes a new PRE (proxy re-encryption) scheme. This scheme is the first unit-directional PRE scheme based on bilinear mapping. It can be applied to secure distributed storage, which shows that the PRE scheme can be used as an effective method to implement secure access control and encrypted data sharing in the file system the proposed system consists of three miners that generate a block of transactions on average every 13 seconds. These miners are running on a Virtual machine with the same hardware capabilities. All the mining devices were configured to use one ethereal wallet that collects the mining reward. These miners are running on with four mining threads each. The Smart Contracts We developed two smart contracts1 on truffle and compiled them with Solidity The first smart contract consists of the functions to register the sensor, request data, and financial functions. The second smart contract is dynamically created in the runtime when the user requests for the data.

### IOT SENSORS

Each sensor TI Sensor tag through Bluetooth Low Energy, as shown in This RSP manages the sensor and the ethereal account to perform transactions on the block chain on behalf of sensors. A sensor application is developed in that connects to the sensor, performs the cryptography functions described in the proxy re-encryption scheme on the sensor data and uploads that data to the cloud storage server. This application synchronizes with the block chain using the Python- JSON-RPC (JavaScript Object Notation - Remote procedure Calls) library. The MAC address of each sensor acts as its identity and is used for re-encryption. Once registered, the sensor starts uploading the encrypted data to the cloud server. It is assumed that the BLE connection between sensor and RSP is completely secure.

### BLOCKCHAIN-BASED DATA SHARING AND ACCESS CONTROL SCHEME

Propose a proxy re-encryption scheme based on block chain. It encrypts the IoT data and stores them in the distributed cloud propose a proxy re-encryption scheme based on block chain. It encrypts the IoT data and stores them in the distributed cloud A customized application is designed as the user interface running on a Raspberry attached to a touch screen. This application uses JSON—RPC to get the sensors' information from the block chain. After selecting the required sensor, the user enters details for specifying the data requirements. We deploy a new smart contract on the block chain in run-time based on the user selected options for the requested data This application keeps track of the Ethereal wallet along with ECC secret key of the data requester. The application downloads the data from the cloud server, checks for the signature and integrity, and decrypts the requested data

### CLOUD STORAGE SERVER

The cloud storage server consists of the RSP and the Google Firebase. RSP acts as ethereal full node and connects to the block chain, while Google Firebase is used for the storage of the data. The authentication and integrity of the data are performed on the RSP and encrypted sensor data along with the Meta data is uploading to the Google

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108133 |

Firebase in JSON format. This cloud also performs proxy re-encryption and updates the smart contract variable for data address sharing.

## IV. ALGORITHMS

### PROXY RE-ENCRYPTION

We measure the impact of proxy re-encryption on the proposed system. The sensor encrypts the data before uploading it to the cloud storage and latherer-encrypts it for sharing the data. The time of the different parts in the scheme is illustrated. As can be seen, it takes on average 48.01 s to share the encrypted data with the user after the initial request with confidence interval of 2.07 s. Consequently, adding proxy-encryption to the scheme increases the delay by 60% due to the mining of the re-encryption key we measure the scalability of the architecture by performing multiple transactions from multiple requesters to the sensor. The whole process was repeated 10times for each scenario before taking the average. In the first scenario, only 1 request was initiated by the user and time was measured from the request to the retrieval of data by the requester. In the latter scenarios, the process was repeated by increasing five requests until the overall request reached high level of results novel block chain based scheme in combination with a proxy re-encryption mechanism to ensure the confidentiality of the data. Here, the advantage of using block chain mechanisms to sell the sensor measurements with different users is that the corresponding financial transactions are automatically managed through the agreed smart contract, stored at the block chain. Moreover, the availability and other quality of service requirements from the legal contract between both parties can be automatically applied. Consequently, compared to the business scenario where the data is stored in a cloud based infrastructure, there is no need for manual verification of the payments and the predefined requirements. Also, disputes on these aspects are completely avoided. The shared data are only visible by the owner and the person present in the smart contract by using a very efficient proxy re-encryption scheme. This novel combination of smart contracts with proxy re-encryption provides a secure platform for the storing and sharing of IoT data.

### BLOCKCHAIN NETWORK:

The block chain network is the critical component of this system. The distribution and sharing of encrypted symmetric key ciphertext depend on the proxy re-encryption mechanism, in which the proxy servers play a vital role. In our system, the block chain consensus node plays the role of proxy servers. The threshold proxy re-encryption scheme is adopted to give better play to the advantage of the decentralization of the block chain network. The DO distribute the multiple shares of re-encryption keys to multiple nodes in the block chain network, respectively. Consensus nodes using the corresponding re-encryption share to re-encrypt the original ciphertext. These converted metadata ciphertexts are collected and packaged into new blocks. In this process, the private key of the data owners and ciphertext information is not leaked into the network. The implementation of this process depends on the block chain consensus algorithm we designed, which is described in detail in the subsequent chapters of this paper. The DU can read the corresponding metadata ciphertext in the block chain ledger. By replacing the third-party semi-honest agent in the proxy re-encryption mechanism with a decentralized block chain network, our method enables reliable and secure encrypted data sharing. All the ciphertext conversion records and data-sharing processes are recorded in the block chain ledger immutably. According to those records, some proxy nodes' malicious access behaviors can be identified easily, which can improve system security.

### STORAGE SERVICE PROVIDERS

The data generated by the IoT devices usually are very massive. Those data collected by IoT devices must be encrypted and uploaded to third-party servers for storing and sharing. Cloud computing and edge computing are widely adapted to store and distribute IoT data. The distributed file system is also a very suitable storage method for storing massive IoT data, such as IPFS. Moreover, the distributed storage service providers can be well combined with a decentralized block chain network, which can improve the security and reliability of encrypted data storage and sharing. In our system, these storage service providers are responsible for storing the user's encrypted IoT data. SSP cannot snoop the plaintext information of the data in the process of data sharing. By separating the grant and authentication of data access from the data storage service, our framework provides a proper way to avoid privacy disclosure to malicious entities

### CONSENSUS ALGORITHM

The consensus mechanism is the core component. Compared with the traditional proxy re-encryption mechanism, our solution utilizes a decentralized network to eliminate dependence on third-party central service

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108133 |

providers. The consensus nodes in block chain networks jointly participate in the consensus process based on re-encrypted ciphertext conversion. The threshold proxy re-encryption can be perfectly combined with the consensus algorithm by splitting and distributing the re-encryption key to the consensus node in the block chain network. The consensus algorithm based on threshold proxy re-encryption, and the following gives a detailed introduction to the consensus mechanism. The consensus mechanism is a core component of the block chain network. Consensus refers to the result that multiple participants who are independent of each other agree on a specific issue. The consensus in the block chain refers to the consistency reached by each node to a certain block in an open decentralized network. The consensus mechanism mainly studies the allocation of accounting rights generated by blocks and the verification after the emergence of blocks the consensus mechanism was first applied in Bit coin. In this consensus mechanism, each node performs a hash operation to compete for the block accounting rights, and after the block is generated, it is broadcast in the whole network for other nodes to verify it. However, the generation of blocks consumes a lot of computing power and other resources, and it takes a long time to achieve data consistency. According to the consensus idea of POW, in our architecture, the process of calculating the hash problem of consensus nodes is replaced by the process of converting ciphertext by using re-encryption keys, and new blocks are generated and written, according to the verification results of other nodes.

## V. CONCLUSIONS

The emergence of the IoT has made data sharing one of its most prominent applications. To guarantee data confidentiality, integrity, and privacy, we propose a secure identity-based PRE data-sharing scheme in a cloud computing environment. Secure data sharing is realized with IBPRE technique, which allows the data owners to store their encrypted data in the cloud and share them with legitimate users efficiently. Due to resource constraints, an edge device serves as the proxy to handle the intensive computations. The scheme also incorporates the features of ICN to proficiently deliver cached content, thereby improving the quality of service and making great use of the network bandwidth. Then, we present a block chain-based system model that allows for flexible authorization on encrypted data.

## REFERENCES

1. R.Karthikeyan, & et all ”Biometric for Mobile Security” in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13552-13555.
2. R.Karthikeyan, & et all ”Data Mining on Parallel Database Systems” in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017,ISSN(0):2361-3361,PP No.:13922-13927.
3. R.Karthikeyan, & et all ”Ant Colony System for Graph Coloring Problem” in the international journal of Engineering Science & Computing, Volume7,Issue7, July2017,ISSN(0):2361-3361,PP No.:14120-14125.
4. R.Karthikeyan, & et all ”Classification of Peer –To- Peer Architectures and Applications “in the international journal of Engineering Science & Computing, Volume7,Issue8, Aug2017, ISSN(0):2361-3361,PP No.:14394-14397.
5. R.Karthikeyan, & et all ”Mobile Banking Services” in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PPNo.:14357-14361.
6. R.Karthikeyan, & et all ”Neural Networks for Shortest Path Computation and Routing in Computer Networks” in the international journal of Engineering and Techniques, Volume3 Issue 4, Aug 2017, ISSN:2395-1303,PP No.:86-91.
7. R.Karthikeyan, & et all ”An Sight into Virtual Techniques Private Networks & IP Tunneling” in the international journal of Engineering and Techniques, Volume 3 Issue 4,Aug 2017, ISSN:2395-1303,PP No.:129-133.
8.R.Karthikeyan, & et all “Routing Approaches in Mobile Ad-hoc Networks” in the International Journal of Research in Engineering Technology, Volume 2 Issue 5, Aug2017, ISSN:2455-1341, Pg No.:1-7.
9. R.Karthikeyan, & et all “Big data Analytics Using Support Vector Machine Algorithm “in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 6 Issue 9, Aug 2018, ISSN:2320 - 9798, Pg No.:7589 -7594.
10. R.Karthikeyan, & et all “Data Security of Network Communication Using Distributed Firewall in WSN ” in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 6 Issue 7, July 2018, ISSN:2320 - 9798, PgNo.:6733 - 6737.
11. R.Karthikeyan, & et all “An Internet of Things Using Automation Detection with Wireless Sensor Network” in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 6 Issue 9, September 2018,ISSN:2320 - 9798, Pg No.:7595 - 7599.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108133 |

12. R.Karthikeyan, & et all “Entrepreneurship and Modernization Mechanism in Internet of Things” in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 7 Issue 2, Feb 2019, ISSN:2320 - 9798, PgNo.:887 - 892.
13. R.Karthikeyan & et all “Efficient Methodology and Applications of Dynamic Heterogeneous Grid Computing” in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 7 Issue 2, Feb 2019, ISSN:2320 -9798, Pg No.:1125 -1128.
14. R.Karthikeyan & et all “Entrepreneurship and Modernization Mechanism in Internet of Things” in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 7 Issue 2, Feb 2019, ISSN:2320 - 9798, PgNo.:887– 892.
15. R.Karthikeyan&etall“Efficient Methodology for Emerging and Trending of Big Data Based Applications” in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 7 Issue 2, Feb 2019, ISSN:2320 - 9798, PgNo.:1246– 1249.
16. R.Karthikeyan & et all “Importance of Green Computing In Digital World” in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 8 Issue 2, Feb 2020, ISSN:2320 - 9798, Pg No.:14 – 19.
17. R.Karthikeyan & et all “Fifth Generation Wireless Technology” in the International Journal of Engineering and Technology, Volume 6 Issue 2, Feb 2020, ISSN:2395–1303.
18. R.Karthikeyan & et all “Incorporation of Edge Computing through Cloud Computing Technology” in the International Research l Journal of Engineering and Technology, Volume 7 Issue 9, Sep 2020 ,p. ISSN:2395–0056, e. ISSN:2395–0072.
19. R.Karthikeyan & et all “Zigbee Based Technology Appliance In Wireless Network” in the International Journal of Advance Research and Innovative Ideas in Education,e.ISSN:2395 - 4396, Volume:6 Issue: 5 , Sep. 2020. Pg.No: 453 – 458, Paper Id:12695.
20. R.Karthikeyan & et all “Automatic Electric Metering System Using GSM” in the International Journal of Innovative Research in Management, Engineering and Technology, ISSN: 2456 - 0448, Volume:6 Issue: 3 , Mar. 2021. Pg.No: 07 – 13.
21. R.Karthikeyan & et all “Enhanced the Digital Divide Sensors on 5D Digitization” in the International Journal of Innovative Research in Computer and Communication Engineering, e-ISSN: 2320 – 9801, p-ISSN: 2320 - 9798, Volume:9 Issue: 4 , Apr. 2021.Pg.No: 1976 – 1981.
22. R.Karthikeyan & et all “Comparative Study Of Latest Technologies In Surface Computing” in the International Journal Of Advance Research And Innovative Ideas In Education, ISSN: 2395-439, Volume:7 Issue: 2 , Apr. 2021. Pg.No: 1540 – 1545.
23. R.Karthikeyan & et all “Crop Yield Prediction Based On Indian Agriculture Using Machine Learning” in the International Journal Of Engineering and Techniques, ISSN: 2395-1303, Volume: 8 Issue: 4, July. 2022. Pg.No: 11 – 22.
24. R.Karthikeyan & et all “A Block chain Approach to Ensuring Provenance to Outsourced Cloud Data in A Sharing Ecosystem” in the International Journal Of Multidisciplinary Research In Science, Engineering and Technology, ISSN: 2584-7219, Volume: 5 Issue:7, July. 2022. Pg.No: 1740 – 1744.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

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