IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

# International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 11, Issue 7, July 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.18

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 7, July 2022||

|DOI:10.15662/IJAREEIE.2022.1107035 |

# A Verifiable and Fair Attribute-Based Proxy Re-Encryption Scheme for Data Sharing in Clouds

**Mr.R.Karthikeyan.,[1] Ms.P.Saranya.,[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:** In web-based overviews, many individuals are not able to give genuine responses because of protection concerns. Consequently, namelessness is significant for online message assortment. Existing arrangements let every part aimlessly mix the submitted messages by utilizing the IND-CCA2 secure cryptosystem. Eventually, all messages are haphazardly rearranged and nobody realizes the message request. Notwithstanding, the weighty computational above and direct correspondence adjusts make it just helpful for little gatherings. In this paper, we propose a productive unknown message accommodation convention focused on a viable gathering size. Our convention depends on a worked on secret sharing plan and a symmetric key cryptosystem. We propose an original technique to allow all individuals furtively to total their messages into a message vector with the end goal that a doesn't part realize anything about other individuals' message positions. We give hypothetical evidence showing that our convention is unknown under vindictive assaults. We then, at that point, lead a careful examination of our convention, showing that our convention is computationally more effective than existing arrangements and results in a consistent correspondence adjusts with a high likelihood.

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

## I. INTRODUCTION

Distributed computing, which gives satisfactory capacity and calculation capacity, has been a common data framework. Rather than overseeing information locally, cloud administrations give an open door to clients reevaluating their information on the cloud without information the board concerns. While it is so helpful to utilize, information security and protection particularly access control on shared information become a worry since the cloud31 administration is typically given by outsiders, for example, the Amazon cloud administrations and cloud. As of late, attribute33based encryption has been adjusted to help adaptable access control on client's accreditation. In an ordinary ABE plot, a client's certification and ciphertext are partner with36 a quality set and an entrance strategy. The ciphertext must be decoded when the trait set fulfills the entrance strategy. Be that as it may; ABE comes up short on capacity of scrambled information sharing which is basic in the circumstance of coordinated effort required. In this manner, characteristic based intermediary re-encryption (ABPRE) was utilized to empower direct change from a ciphertext to another. And all the cloud server necessities to manage is the encoded information and a re-encryption key. The ciphertext under one strategy would be changed by re-encryption to a new ciphertext partner with another arrangement. During the change, the cloud server can't uncover the fundamental plaintext. In such a way, the beneficiary with access strategy P1 can impart its re-appropriated encoded information to a common client with access strategy P2. Nonetheless, a main pressing concern of ABPRE is that the beneficiary can't guarantee the legitimacy of the re-scrambled ciphertext returned by the cloud server. Since the re-encryption calculation's intricacy is direct with the size of the entrance strategy, the calculation can be over the top expensive. Thus, the cloud server might reuse a formerly produced re-encoded ciphertext or even an irregular re-scrambled ciphertext to save its calculation asset. Besides, the ongoing ABPRE plans can't accomplish the decency property which keeps the cloud server from a malevolent allegation of returning a mistaken re-encoded ciphertext on the off chance that it has without a doubt acted really the cloud server can re-scramble the first ciphertext to a common client's ciphertext.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 7, July 2022||

|DOI:10.15662/IJAREEIE.2022.1107035 |

The worry is that the common client can't guarantee that the returned re-encoded ciphertext is a right re-scrambled ciphertext of the first ciphertext. The cloud server might return a mistaken re-encoded ciphertext to save its calculation cost. Wrong genome information might prompt a debacle to the examination result. That's what another issue is, the common client might blame the cloud serve for returning a wrong re-encoded ciphertext regardless of whether the re-scrambled ciphertext is right. Thusly, the common client might decline to pay for the cloud administration which is a basic issue for the business cloud administration framework. From the get go, one might figure this issue can be settled through checking the re-encryption assuming the server distributes the re-encryption key and the first ciphertext. Thusly, everybody can rehash the re-encryption activity to confirm the rightness of the ciphertext returned by the server. Nonetheless, such a way is illogical as the re-encryption activity cost is costly; it isn't appropriate for a verifier to rehash this calculation expensive work. Another unimportant arrangement is that a common client can uncover his confidential key so the first beneficiary can decode the returned re-encoded ciphertext and afterward he can approve the plaintext is unique. Notwithstanding, uncovering private key might bring about basic security issues to the common client.

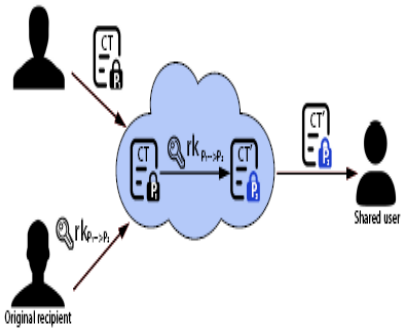



**Fig 1 System Architecture**

## II. LITERATURE REVIEW

The Data Producer Domain contains those elements that create information. Since age doesn't infer proprietorship, the differentiation between information maker and information proprietor becomes vital. In any case, information makers can take part in the assurance of the information all along, by scrambling it from the source, and send it straightforwardly to the capacity supplier, in this way decoupling this collaboration from the information proprietor. The Data Owner Domain is fixated regarding the matter that possesses the information whose entrance is to be appointed. The primary capability of the information proprietor is to approve purchasers to get to his information. Note that the information proprietor can likewise (and most times does) go about as an information maker, however this doesn't preclude situations where separate substances partake in information creation (e.g., informatio proprietor's gadgets). We expect that the information proprietor connects with different entertainers through a client specialist, typically a program or a particular application, running on a confided in PC. This area is thought to be totally confided in by the information proprietor. The Secure Storage Provider Domain is constrained by specific substances that steward information proprietors' data and give a safe access administration, without having the option to learn anything. Considering that distributed computing is the most unmistakable launch of the thought about situation; we will likewise allude to this entertainer as the cloud supplier. This space is thought to be semi trusted, since we expect that the supplier will offer the support accurately, in any case, simultaneously, it might have impetuses for attempting to peruse the information. This trust supposition that is made sense of underneath in more detail. The Data Consumer Domain involves the substances that are authentic beneficiaries of the data shared by the information proprietor, which incorporate individuals, yet in addition outsider administrations and information proprietor's gadgets. Shoppers access this data through the capacity administration given by the cloud.

Attribute-based encryption (ABE) is a public-key-based one-to-numerous encryption that permits clients to scramble and unscramble information in light of client credits. A promising utilization of ABE is adaptable access control of scrambled information put away in the cloud, utilizing access polices and credited credits related with private keys and ciphertexts. One of the primary effectiveness disadvantages of the current ABE plans is that decoding

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 7, July 2022||

|DOI:10.15662/IJAREEIE.2022.1107035 |

includes costly matching activities and the quantity of such tasks develops with the intricacy of the entrance strategy. As of late, Green et al. proposed an ABE framework with rethought decoding that generally kills the unscrambling above for clients. In such a framework, a client gives an untrusted server, say a cloud specialist co-op, with a change key that permits the cloud to decipher any ABE ciphertext fulfilled by that client's credits or access strategy into a straightforward ciphertext, and it just causes a little computational above for the client to recuperate the plaintext from the changed ciphertext. Security of an ABE framework with rethought decoding guarantees that a foe (counting a malevolent cloud) can not learn anything about the scrambled message; nonetheless, it doesn't ensure the rightness of the change done by the cloud. In this paper, we think about another necessity of ABE with re-appropriated decoding: unquestionable status. Casually, evidence ensures that a client can productively check assuming that the change is done accurately. We give the conventional model of ABE with unquestionable reevaluated unscrambling and propose a substantial plan. We demonstrate that our new plan is both secure and irrefutable, without depending on irregular prophets. At long last, we show an execution of our plan and consequence of execution estimations, which demonstrates a critical decrease on registering assets forced on clients.

To oversee reevaluated encoded information partaking in mists, trait based intermediary re-encryption (ABPRE) has turned into an exquisite crude. In ABPRE, a cloud server can change a unique beneficiary's ciphertext to another one of a common client's. As the change is calculation consuming, a malevolent cloud server might return a mistaken re-encoded ciphertext to save its calculation assets. Besides, a common client might blame the cloud server for returning an erroneous re-encoded ciphertext to decline to pay the expense of utilizing the cloud administration. In any case, existing ABPRE plans don't uphold a system to accomplish evidence and reasonableness. In this paper, a clever evident and fair quality based intermediary re-encryption (VF-ABPRE) plot is acquainted with help evidence and decency. The unquestionable status empowers a common client to check whether the re-encoded ciphertext returned by the server is right and the decency guarantees a cloud server escape from vindictive allegation in the event that it has without a doubt led the re-encryption activity sincerely. Furthermore, we direct a presentation trial to show the proficiency and common sense of the new VF-ABPRE plot.

Distributed computing offers a colossal asset pool by concentrating different assets with the quick development of computerized information. Information capacity is the most satisfactory help in distributed computing. As one of the vital advances of distributed storage administration, information reduplication innovation permits cloud servers to save extra room by erasing repetitive information. To safeguard information protection, information holders for the most part scramble their information first, and afterward transfer the encoded information to the cloud server, which obviously brings another test for cloud information reduplication, as conventional reduplication innovation can't reduplicate encoded information. Existing arrangements have different security issues. They can't deftly uphold information access control, and furthermore require information clients to stay on the web. In this paper, we propose character based intermediary re-encryption information reduplication conspire utilizing personality based intermediary re-encryption (IB-PRE) and personality based verification of possession (IB-PoW). The proposed plot incorporates cloud information reduplication with access control. By nitty gritty security investigation and execution assessment, we show that the proposed conspire is security, productive and viable.

## III. METHODOLOGIES

To play out an intensive survey on PRE plans and applications, we followed a philosophy to distinguish and channel distributions in view of bibliometric models. A far reaching reference index on PRE plans and applications, painstakingly kept up with by Shao, filled in as a first crude cause of distributions. What's more, we physically added a few important distributions began from our own investigation of the writing or from questions for pertinent catchphrases to web search tools. The aftereffect of this stages two arrangements of distributions, one zeroed in on plans (83 papers) and the other on applications (69 papers). Then, it was important to channel the rundown of PRE plans, given the responsibility related to their investigation. Albeit, as a general rule, a large portion of the papers were to begin with contemplated, some of them were sifted through. We involved the quantity of destinations for each paper, as estimated by Google Scholar, as a heuristic measurement of the importance of the paper. For example, non-late distributions (e.g., before 2009) which have no refers to yet, were set apart as not applicable. Nonetheless, manual confirmation of the disposed of distributions was expected to dispose of misleading negatives. Note that we zeroed in solely in standard PRE plans, precluding different variations (e.g., restrictive, declaration less, broadcast, and so on) that suggest solid changes to the linguistic structure, security ideas and properties, which makes examinations less significant. Intermediary Re-Encryption (PRE) is a sort of open key encryption that permits an intermediary substance to change ciphertexts starting with one public key then onto the next, without picking up anything about the fundamental information. Subsequently, according to a practical perspective, it very well may be viewed for of sharing

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 7, July 2022||

|DOI:10.15662/IJAREEIE.2022.1107035 |

information safely. The center propose of this paper is that intermediary encryption is an excellent possibility to develop cryptographically upheld access control frameworks where the safeguarded information is put away remotely, since it empowers dynamic designation to scrambled data. In a PRE-based arrangement, confidential information can dwell in the cloud in scrambled structure and be shared to approved clients through re-encryption, while as yet staying classified concerning unapproved parties and the cloud supplier itself

**THE SECURE ACCESS DELEGATION SCENARIO**

The requirement for debilitating the conventional security suspicions that administer the ongoing security models of cloud frameworks makes the encryption of information before re-appropriating a fundamental necessity. Simultaneously, it is additionally important that the executed encryption methods permit appointing access for the end goal of sharing, which is quite possibly of the most essential usefulness. We allude conventionally to this setting as the safe access designation situation. There are, truth be told, further developed functionalities, for example, looking, or in any event, figuring, over encoded information; yet, the entrance appointment usefulness is extremely difficult as the dispersion of access privileges becomes troublesome once the data has been scrambled and rethought. In any entrance assignment situation (whether or not there is re-appropriating or not), there are three principal separate jobs: information makers, information proprietor, and information buyers. The most nonexclusive utilization connection in this setting is that various information makers produce information which is claimed by an information proprietor, who turn can impart it to numerous information purchasers. A significant part of this utilization connection is that the information proprietor and information makers can be independent elements, not really inside a similar security space. This last trademark has extraordinary ramifications with regards to planning secure, yet versatile, arrangements, since these guidelines out ordinary methods, for example, the utilization of public-key encryption alone. Likewise, under our rousing situation, we likewise present a fourth job that gives an information stockpiling administration, where data is scrambled. Figure 1 portrays these jobs and areas, as well as the connections and co operations between them

The Data Producer Domain contains those substances that create information. Since age doesn't infer possession, the differentiation between information maker and information proprietor becomes important. Notwithstanding, information makers can take part in the security of the information all along, by scrambling it from the source, and send it straightforwardly to the capacity supplier, in this way decoupling this association from the information proprietor.

The Data Owner Domain is fixated regarding the matter that possesses the information whose entrance is to be designated. The principal capability of the information proprietor is to approve shoppers to get to his information. Note that the information proprietor can likewise (and most times does) go about as an information maker, yet this doesn't preclude situations where separate substances take part in information creation (e.g., information proprietor's gadgets). We expect that the information proprietor connects with different entertainers through a client specialist, typically a program or a particular application, running on a confided in PC

The Secure Storage Provider Domain is constrained by particular substances that steward information proprietors' data and give a safe access administration, without having the option to learn anything. Considering that distributed computing is the most unmistakable launch of the thought about situation; we will likewise allude to this entertainer as the cloud supplier. This space is thought to be semi trusted, since we expect that the supplier will offer the support accurately, yet, simultaneously, it might have motivations for attempting to peruse the information. This trust supposition that is made sense of howling more detail.

The Data Consumer Domain contains the substances that are authentic beneficiaries of the data shared by the information proprietor, which incorporate individuals, yet additionally outsider administrations and information proprietor's gadgets. Shoppers access this data through the capacity administration given by the cloud.

## IV. ALGORITHMS

**ATTRIBUTE-BASED PROXY RE-ENCRYPTION**

In ABPRE, a cloud server can change a unique beneficiary's ciphertext to another one of a common client's. As the change is calculation consuming, a noxious cloud server might return a mistaken re-scrambled ciphertext to save its calculation assets. Besides, a common client might blame the cloud server for returning a wrong re scrambled ciphertext to decline to pay the expense of utilizing the cloud administration. In any case, existing ABPRE plans don't uphold a system to accomplish obviousness and reasonableness. As a matter of fact a third storage space is difficult to come by. The shaking and rearranging exercises are under the entirety of individuals' reconnaissance, which is challenging to carry out in a dispersed organization. The cloud server of returning a mistaken re encoded ciphertext to decline to pay the expense of utilizing the cloud administration. ABPRE plans don't uphold a component to accomplish evidence and reasonableness.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 7, July 2022||

|DOI:10.15662/IJAREEIE.2022.1107035 |

## SECURITY MODELS OF PROXY RE-ENCRYPTION

Being intermediary re-encryption an expansion of public-key encryption, it is normal that the security models for PRE expand those of PKE. In any case, the capacity to re-encode ciphertexts presents a fascinating test while confronting the meanings of safety for PRE. From one perspective, PRE developments need to ensure the security targets of the plan, for example, privacy and legitimacy of ciphertexts. Then again, they need to permit the re-encryption of ciphertexts. Naturally, the two objectives appear to struggle with one another.. An early idea, suggestive of intermediary re-encryption, was introduced in 1997 by Mambo and Okamoto in spite of the fact that their proposition inferred that the first beneficiary should be accessible for re-encoding ciphertexts when required, which isn't doable all the time. Blast, Bloomer and Strauss proposed in 1998 the main intermediary re-encryption plot, which agrees with the laid out idea of intermediary re-encryption. From that point forward various plans have been proposed. In this Section we survey a choice of these plans. To appropriately recognize plans, each plan was marked with the creator's initials and year of distribution, and if vital, an extra alphabetic file to recognize plans inside a similar distribution.

## SECURITY NOTIONS FOR PRE

Comparatively to PKE, the most regular security ideas in Prepare in recognize capacity against picked plaintext assaults (INDCPA) and in recognize capacity against picked ciphertext assaults (IND-CCA) the two thoughts catch the powerlessness of an enemy to recognize ciphertexts for known messages, and vary from one another by when the prophets are free for the foe. These security thoughts are officially characterized as a two-stage security game: during the principal stage, the enemy cause the accessible prophets, compelled by certain circumstances; next, before the subsequent stage begins, the foe unreservedly picks two messages and gets the test ciphertext, which is an encryption of one of them indiscriminately; next, he can utilize the accessible prophets, once more, obliged by certain circumstances; lastly, he needs to figure which of the messages was scrambled

## LIMITED MULTI-USE SCHEMES

While the past sorts of multiuse plans support an endless number of re-encryptions, some new intermediary re-encryption plans, specifically those in light of grids [6, 7, 8, 9], present a restricted variant of topical use property, since the re-encryption capability acquaints commotion with the ciphertext. Consequently, and contingent upon the boundaries utilized, the gathered commotion makes the decoding methodology to flop after a specific number of re-encryptions. This might try and occur after only one re-encryption. Subsequently, plans of this sort are in a middle of the road region between single-use and multi-use. For example, the plan from Nunez ˜ et al. is of this sort, as the quantity of conceivable re-encryptions fluctuates with the boundaries utilized; specifically, the typical number of re-encryptions that is upheld changes from 5 to 50. Another intriguing model is the plan from Kirshanova, which is purportedly single-use, albeit that would eventually rely upon the selection of boundaries.

## V. CONCLUSIONS

This paper presents the evidence and decency security necessities for quality based information partaking in mists and set forward a thought of obvious and fair ciphertext-strategy property based intermediary re-encryption (VF-CP-ABPRE).The conspire gives the capacity to a common client to confirm the legitimacy of the re-scrambled ciphertext. Besides, a common client can't make a vindictive allegation to the cloud supplier on the off chance that the cloud has to be sure returned a right re-encoded ciphertext. We additionally have demonstrated our VF-CP-ABPRE plan's semantic security, obviousness and reasonableness in our security model. We 808also directed an execution to assess our proposed plot, and thought about the execution time between our plan and past plans to exhibit the productivity of the proposed VF-CP-ABPRE conspire.

## REFERENCES

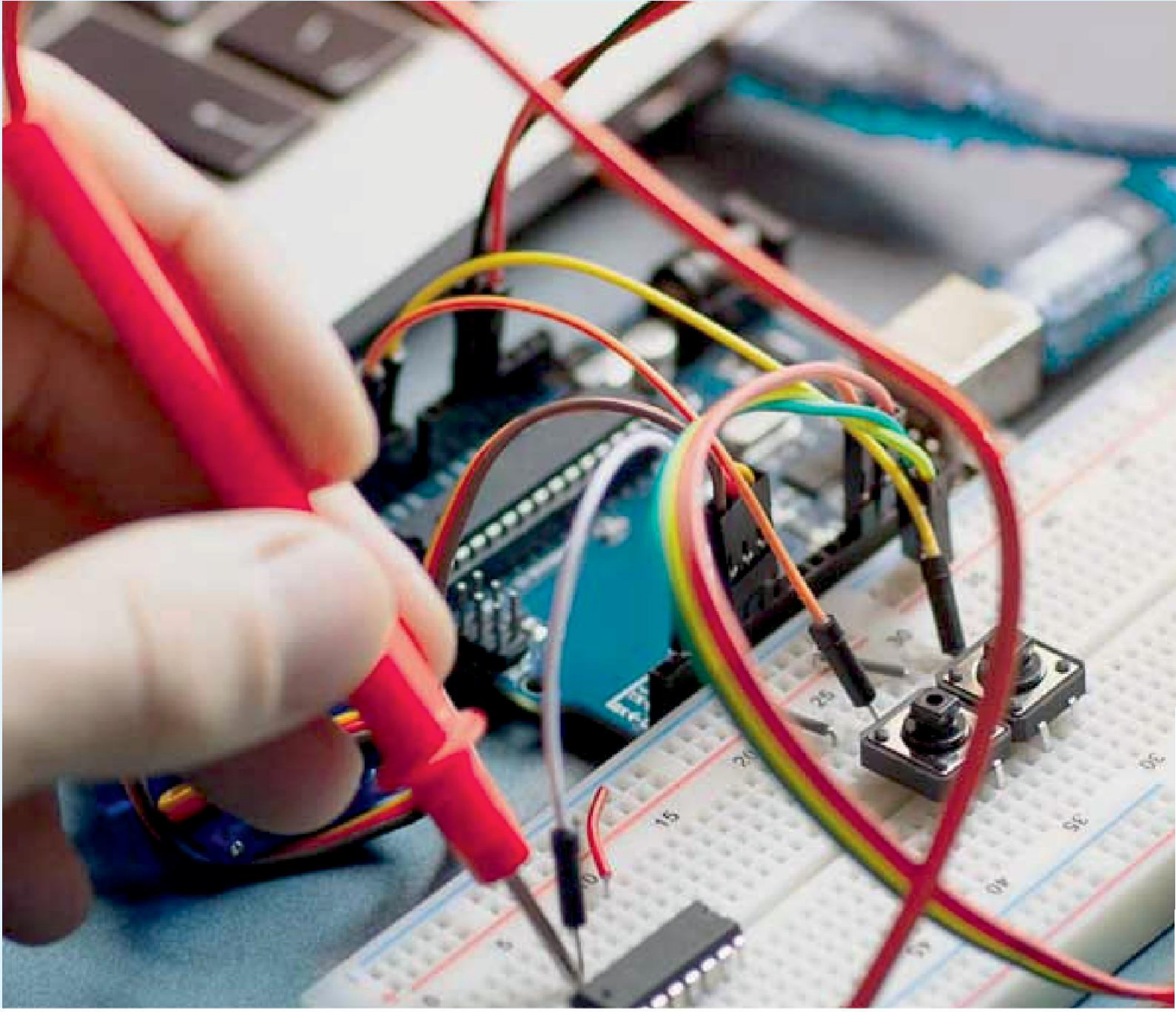
1. R.Karthikeyan, & et all ”Biometric for Mobile Security” in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13552-13555.
2. R.Karthikeyan, & et all ”Data Mining on Parallel Database Systems” in the international journal of Engineering 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, July 2017, 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, Aug 2017, 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,PP No.:14357-14361.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 7, July 2022||

|DOI:10.15662/IJAREEIE.2022.1107035 |

6. R.Karthikeyan, & et all ”Neural Networks for Shortest Path Computation and Routing in Computer Networks” in the international journal of Engineering and Techniques, Volume 3 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, Aug 2017, 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, Pg No.: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.
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, Pg No.: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, Pg No.: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, Pg No.: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 Blockchain 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

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

**Impact Factor: 8.18**

# International Journal of Advanced Research

## in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

www.ijareeie.com

Scan to save the contact details