International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.48047/INTJECSE/V15I4.67 ISSN: 1308-5581 Vol 15, Issue 04 2023

Data Duplication Removal Technology Using AWS Services

1 Mrs. SRILATHA PULI,
Assistant Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India, srilatha.puli@sreyas.ac.in
2 Chenemilla Sathvik
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India, sathvikchenemilla@gmail.com
3 Chilakapati Srikar
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India, chilakapatisreekar1112@gmail.com
4 Mudrakolla Pragathi
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India, pragathi.vppr@gmail.com
5 Pulapalli Sriyashveer Reddy
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India, sriyashveer@gmail.com

ABSTRACT: Cloud computing comes all through core interest advancement of network computing, virtualization just as web advancements. With an expansion in the use of cloud storage, powerful strategies should be utilized to diminish equipment costs, meet the data transmission necessities, and build stockpiling proficiency. This can be accomplished by utilizing Data Deduplication. Using this, less information will be on the server thus require less equipment and users would have the option to put more data in the additional space available. At present utilization of cloud storage is expanding and to conquer expanding information issues, Data deduplication methods are utilized. Information Deduplication methods can't be applied straightforwardly with security instruments. In this paper, we are eliminating copy information to save storage space and speed up the organization. Here we applied MD5 hashing to generate a hash value (when uploaded to cloud storage) and then compare those with values (when the same file uploaded with a different name) to find out the duplicate data in the cloud environment. When deduplication is accomplished, a framework plan for secure information changes in the organization. Security is accomplished through encryption and decoding of the information. This paper inspects secure deduplication strategy. After removal of duplicate data pointers will give reference to the original file.
Keywords – *Cloud Computing, MD5 hashing algorithm, AWS Services, Data Deduplication*

1.INTRODUCTION

Cloud computing utilizes several methods in PaaS, a great application advancement stage for the designer to make web based applications. Inside IaaS processing framework can be shipped off as an assistance towards the requester. In your present application structure related to Virtual Machine (VM).Cloud computing is still under the turn of events stage and has many issues notwithstanding challenges out of a few inquiries in cloud planning assumes a vital part inside deciding your current powerful execution. Computerized applications are developing quickly and utilization of the cloud in the web has expanded quickly. Cloud gives a few advantages in terms of cost and on-interest administrations. Genuine-time correspondence like PCs received different figuring structures and distributed computing. Presently day's most extreme measure of information is put away in cloud climate because of capacity also, organizing climate. Information plate can't perceive the copied information that shows up on the plate. Copying information can influence the extra room of the circle. Copy information shows up when a normal method is utilized to store and address the information. Identification of duplication information is tedious. Essentially Data has been grouped into two kinds in particular 'organized information' and 'unstructured information which are assuming a significant part in the ongoing pattern. Typically the construction information can be effectively coordinated incorporating site log information, client call point by point records, and so on. Due to the fast increment of web-based media use and portable utilization, the unstructured information can't be handily coordinated incorporates blog information, web-based media

collaboration information, recordings, and so forth, So, unstructured information ought to be overseen practically. Today in IT spending plans, on a normal of 13% of the cash being contributed to capacity1. These effects make more issues, similar to the debasement of execution, bargain of value, and more operational expenses. So to beat the above issues and handle the framework where the idea of Deduplication is determined. Deduplication innovation investigates information either at a square level (subrecord) or document level. The approaching information is parted into more modest fixed or variable squares or sections. Every one of these more modest squares is given an extraordinary identifier which is made by a few hashing calculations or even a little by little correlation of the square. Normal calculations utilized for this cycle are MD5. Additionally, content mindful rationale, which thinks about the substance of the information and concludes the size of squares and limits. As the deduplication framework measures information, it looks at the information to the all-around recognized squares and stores it in its information base. If a square as of now exists in the information base, the new excess information is disposed of and a reference to the current information is embedded into the vault. If the square contains new, novel information, at that point the square is embedded into the information store (document framework). The essential advantage of deduplication is that it incredibly diminishes capacity limit prerequisites, drives a few different points of interest like rescued power utilization, reduced cooling prerequisites, longer circle-based maintenance of information (quicker recuperation), and debacle recuperation.

2. LITERATURE SURVEY

A review of cloud computing security issues.

Cloud computing technology is an old concept which has become one of the most widespread technologies in the last few years. It is a pay-per-use service which enables users to perform computing services anytime and anywhere as long as an internet connection is available. There are four major cloud deployment models: public, private, community and hybrid. The cloud’s prominence originates from its valuable advantages. However, security issues threatening data confidentiality, integrity, availability and auditing in the cloud might hamper this technology diffusion. Thus, deciding whether or not to move to a cloud service provider, or rely on available IT resources to run a business, is indeed a critical step. This paper presents an overview of cloud computing and describes this technology in detail. It also summarizes most of the current security issues menacing the cloud providers and users, and presents and summarizes the available countermeasures to the proposed security issues.

Tech Learning Community Management

An overview of the characteristics of professional learning communities (PLCs), found that the impact of PLCs on teaching practices and student learning is positive. A small number of empirical studies explore the impact on teaching practice and student learning.so the working on teaching and learning practice is in effect. So we are going to introduce a new community that provides online learning, teaching and achievements on empirical studies. The collective results of these studies will suggest that teaching practice and student achievements. Implications of this project and suggestions for next steps in the efforts to document the impact of PLCs on teaching and learning are included.

A Survey on ETS Using Android Phones.

The Rapid growth of android applications is creating a great impact on our lives. The aim of this survey Employee monitoring system using android mobile is, to automate the employee monitoring process in company by their Employee's office cell phone and also improve the organizational growth of the company. In this paper, we discuss the design and Implementing admin application, employee application and Centralized server for monitored company employee's using android technology. In this system we are providing a dynamic database utility which retrieves data or information from a centralized database. The android application in smartphone contains all information about the employee phone uses like their all Employee S MS history, Employee call Logs, Employee Locations, Data uses, Web browser history, and unauthorized data uses details. All communication between the Employee phone and the admin is done through 3G network technology. This application is user-friendly. This system improves accuracy in managing employees of the company by saving time, reducing manager efforts; avoid the unnecessary use of company phones which are provided to the

Employee for their office use only. This System is also connected to the centralized server for accessing detailed history of employee phone uses. The main aspect of our paper is that Managers can navigate their all company Employees through mobile phones and know the employee behavior (Good-Loyal/Average/Bad).

Reconciling end-to-end confidentiality and data reduction in cloud storage.

An increasingly common practice for users of storage systems is to perform end-to-end encryption to ensure the confidentiality of data stored on external storage systems or in the cloud. This practice, however, inhibits the benefits of deduplication and compression performed downstream from where data is encrypted; as a consequence, the required storage capacity increases, and so does the overall cost of the service. In this paper, we address this problem by proposing a framework that reconciles end-to-end encryption with downstream compression and deduplication. The proposed framework guarantees the confidentiality of data in transit and at rest, even after clients cancel a cloud storage subscription, without affecting the ability of storage systems to perform data reduction functions. The framework requires only minor modifications in storage applications that encrypt data, and no changes in a client's business applications. Additionally, we propose several secure data reduction algorithms to compress and deduplicate data without compromising its confidentiality, even if the data is originally encrypted with different keys. We present a comprehensive security analysis that shows that the framework is secure against malicious cloud administrators, other tenants and law enforcement agencies. Our prototype shows that, for a reasonable extra overhead in the time required to store data, the framework enables a considerable amount of storage capacity savings.

A novel encryption scheme for data deduplication system

In order to solve the problem that encryption files can not benefit from the data deduplication technology, a novel encryption scheme is proposed. According to the method, the basic encryption unit is transformed from the file to the chunks; and the chunk contents are used to generate the symmetric keys, which ensure the determinate mapping between plaintext and ciphertext of data. The data can be stored and transmitted in security as long as the adversary does not acquire a user's private key and identification password simultaneously. This scheme can mitigate the contradiction between traditional encryption method and deduplication technology well; and is suitable for the application of disk-based, data deduplication systems which has the requirement of confidentiality.

Reclaiming space from duplicate files in a serverless distributed file system

The Farsite distributed file system provides availability by replicating each file onto multiple desktop computers. Since this replication consumes significant storage space, it is important to reclaim used space where possible. Measurement of over 500 desktop file systems shows that nearly half of all consumed space is occupied by duplicate files. We present a mechanism to reclaim space from this incidental duplication to make it available for controlled file replication. Our mechanism includes: convergent encryption, which enables duplicate files to be coalesced into the space of a single file, even if the files are encrypted with different users' keys; and SALAD, a Self-Arranging Lossy Associative Database for aggregating file content and location information in a decentralized, scalable, fault-tolerant manner. Large-scale simulation experiments show that the duplicate-file coalescing system is scalable, highly effective, and fault-tolerant.

A secure cloud backup system with assured deletion and version control.

Cloud storage is an emerging service model that enables individuals and enterprises to outsource the storage of data backups to remote cloud providers at a low cost. However, cloud clients must enforce security guarantees of their outsourced data backups. We present Fade Version, a secure cloud backup system that serves as a security layer on top of today's cloud storage services. Fade Version follows the standard version-controlled backup design, which eliminates the storage of redundant data across different versions of backups. On top of this, Fade Version applies cryptographic protection to data backups. Specifically, it enables fine-grained assured deletion, that is, cloud clients can assuredly delete particular backup versions or files on the cloud and make them permanently inaccessible to anyone, while other versions that share the common data of the deleted versions or files will remain unaffected. We implement a proof-of-concept prototype of Fade Version and conduct empirical evaluation atop Amazon S3. We show that Fade Version only adds minimal performance overhead over a traditional cloud backup service that does not support assured deletion.

3. PROPOSED ARCHITECTURE

Present day information duplication is a quickly developing method used in information reinforcement stored without excess. It is vital, special and unique. In this paper, we design an interactive protocol using AWS services in which we use the AWS lambda function for generating the hash value of the file which gets uploaded. We use AWS cloud watch for records of every file, and also use the S3 bucket for storing and retrieving the data. We investigated the information to decide the relative adequacy of information deduplication, especially considering the entire record versus the block-level end of excess. Security in information deduplication can be furnished with the utilization of a concurrent encryption method that encodes the information previously transferred to the public framework. To prove the thought, we proposed the model and attempted some tests, in that test we uploaded the same files with different names and different file systems such as pdf, doc, odt. The work shows that the proposed system works correctly and gives a warning that the same file was uploaded before. Cloud computing is productive and adaptable yet keeping up the strength of preparing such countless positions in the distributed computing climate the cloud framework faces the issues of replication furthermore, the information duplication as indicated by situations. In this setting we need to tackle the issue of both, to upgrade the cloud execution as far as capacity overhead and accessibility needed to deal with the whole information in such a way by which the hunting capacity and the ordering of information can be accomplished both.

A. DATA DEDUPLICATION WORKING

Data deduplication works by seeing items (ordinarily records or then again squares) and dispenses with objects (copies) that as of now exist in the educational assortment. All the cycles which are not uncommon are taken out in this method. In the Data deduplication procedure, we parcel the data into blocks, and hash regard is resolved for all of these squares. By then using these hash regards we can choose if another square of similar data has recently been taken care of. If a commensurate information report is found, reject the copy information with a reference to the article satisfactorily present in the educational record.The process of deduplication is shown in Figure 1

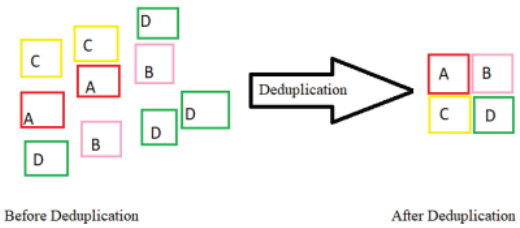

Fig. 1. Deduplication Process

B. HASH BASED ALGORITHM

Hash-based deduplication systems use counts to perceive chunks of data. In case the hash is currently made, the data is perceived as a duplicate and isn't taken care of. Message Digest Algorithm 5(MD5): This 128-cycle is in the manner expected for cryptographic jobs. In this strategy, the 128-cycle state is divided into four 32-bit words, implied A, B, C, and D. These are acquainted with certain fixed constants. This cycles the "knot" with hashing estimation to make a hash. If the hash as of now exists, the data is viewed as a duplicate and isn't taken care of. If the hash doesn't exist, by then the data is taken care of and the hash record is revived with the hash. The hashing procedure is depicted in Figure 2.

C. DEDUPLICATION IMPROVED TECHNIQUE

Deduplication is a suitable strategy for the headway of instances of data set aside in disseminated capacity. Deduplication can be requested into lumps level and report level deduplication. Pieces level deduplication procedure approves the limit of uncommon irregularities by taking a gander at each

moving toward the piece for duplicate ID. This methodology achieves better deduplication viability since it requests deduplication.

D. Proposed Approach

The examination issue in this paper requires the utilization of quantitative techniques for estimating, positioning, arranging, distinguishing examples, and making speculations. We want to find a way to give each file and unique hash ID stored in the Amazon S3 bucket and use that id to compare with the newly uploaded/collected files. Another Lambda Function to successfully implement the Data Deduplication. The proposed approach is depicted in Figure 3.

1. $R = readDocument(D)$
2. $E = extractTextFeaters(R)$
3. $IM.createEntry(E)$
4. $E = EncryptData(R)$
5. $Sp[] = E.splitFile(E)$
6. $for(i = 0; i \leq Sp.length; i++)$
    a. $H = genrateHash(Sp[i])$
    b. $if(H != HashTree.node)$
        i. $HashTree.createNode(H)$
    c. Else
        i. Remove H
    d. End if
7. End for

Fig. 2. Hashing Procedure

Fig. 3. Proposed Approach

As the figure shows, the data can be collected from used smartphones or desktops. Once the data has been uploaded on the primary bucket, a trigger will be launched to run the first lambda function. The purpose of Python Code executing in AWS Lambda function regularly would be to generate the unique HASH of the data object uploaded by the user and second python code executing in an AWS Lambda function to compare that hash value with all other hash values available in the DynamoDB

table for fast and predictable performance with seamless scalability. If the Python code executing in the second AWS Lambda Function did manage to find a hash already available in the table, it will increment the count column by 1 else it will make a new entry for the new hash value. If the count column value is greater than 1 it will not upload the file in the Final Amazon S3 bucket.

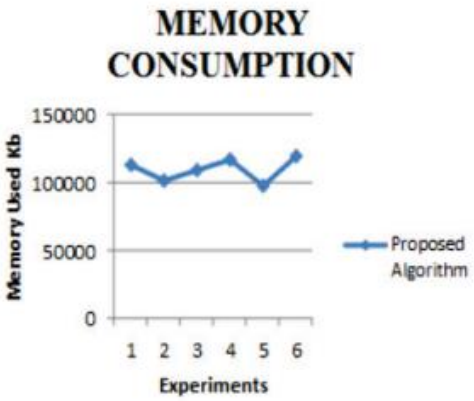

Fig. 4. Memory Consumption

4. EXISTING SYSTEM

To study the data breaches in cloud storage, a study was carried by. Various instances of breaches were found where the data of the client was exposed by the service providers. The instances exposed that if the service provider or the client has access to data of other users the breaching of data was more. For handling the data breach problem, the authors suggested end-to-end encryption. The issues in deduplication while encryption were found by authors in. To resolve them they proposed a novel encryption methodology. In the methodology, the encryption units were transformed into chunks and these chunks were used to produce symmetric keys. The symmetric key obtained were used to limit mapping between plain and ciphertext. To reclaim space that was lost during replicating files, a methodology was introduced by. The methodology involved convergent encryption that permitted duplicate files to be consolidated into a single file using diverse user keys and SALAD, a Self Arranging Lossy Association Database.

5.RESULTS

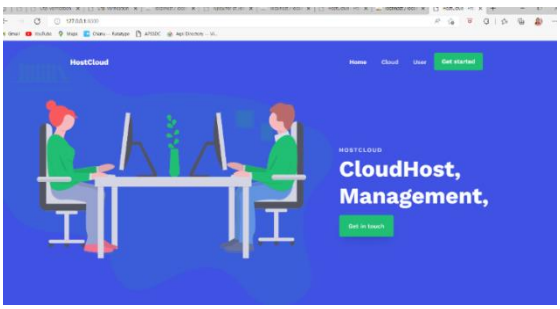

Fig 1: Landing page

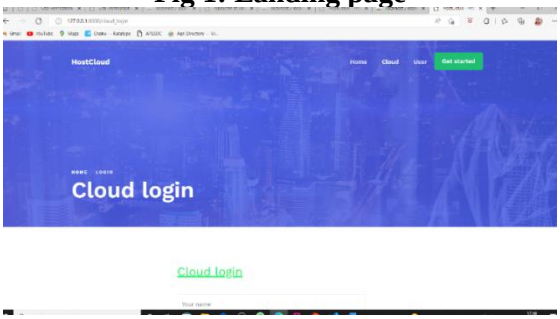

Fig 2: Cloud Login

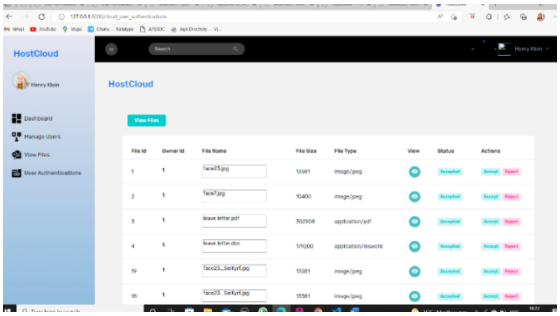

Fig 3: User Authentication

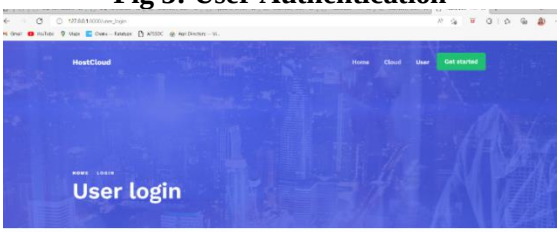

Fig 4: User Login

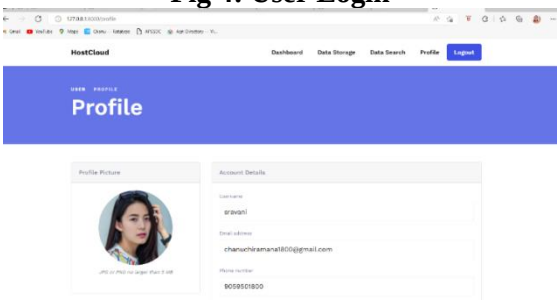

Fig 5: User Profile

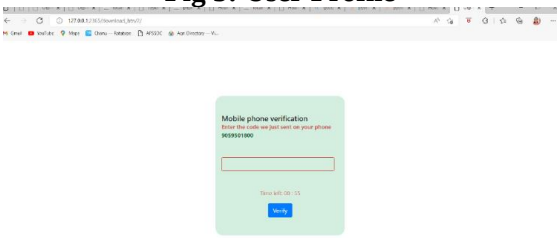

Fig 6: Verification

6. CONCLUSION

This paper would be helpful to new examiners who need to investigate secure data deduplication Security procedures amassed here in future we work to improve the execution of our proposed work in security prospect. A fundamental technique that makes deduplication suitable with mixed data. A methodology needs to be pursued for data duplication and secure transmission over a disseminated processing environment. We work for another security approach for secure data transmission utilizing AWS benefits additionally, a deduplication framework using one of the hashing calculations MD5.

7. REFERENCES

[1] Bhoyar, R., & Chopde, N. (2013). Cloud computing: Service models, types, database and issues. International Journal of Advanced Research in Computer Science and Software Engineering, 3(3).

[2] Kaur, M., & Singh, H. (2015). A review of cloud computing security issues. International Journal of Advances in Engineering & Technology, 8(3), 397.

[3] Pathan, A. I. (2017). Proposed: Tech Learning Community Management. International Journal for Scientific Research & Development (IJSRD) Vol, 5, 2321-0613.

[4] Pathan, A. I., & Shaikh, S. H. (2018). A Survey on ETS Using Android Phones. International Journal Of Innovative Research In Technology (IJIRT), 5(3).
[5] Baracaldo, N., Androulaki, E., Glider, J., & Sorniotti, A. (2014, November). Reconciling end-to-end confidentiality and data reduction in cloud storage. In Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security (pp. 21-32).
[6] Wang, C., Qin, Z. G., Peng, J., & Wang, J. (2010, July). A novel encryption scheme for data deduplication systems. In 2010 International Conference on Communications, Circuits and Systems (ICCCAS) (pp. 265-269). IEEE.
[7] Douceur, J. R., Adya, A., Bolosky, W. J., Simon, P., & Theimer, M. (2002, July). Reclaiming space from duplicate files in a serverless distributed file system. In Proceedings 22nd international conference on distributed computing systems (pp. 617-624). IEEE.
[8] Rahumed, A., Chen, H. C., Tang, Y., Lee, P. P., & Lui, J. C. (2011, September). A secure cloud backup system with assured deletion and version control. In 2011 40th International Conference on Parallel Processing Workshops (pp. 160-167). IEEE.
[9] SRILATHA PULI, A MACHINE LEARNING MODEL FOR AIR QUALITY PREDICTION FOR SMART CITIES, DESIGN ENGINEERING || ISSN: 0011-9342 | YEAR 2021 - ISSUE: 9 | PAGES: 18090 – 18104
[10] SRILATHA PULI, QUALITY RISK ANALYSIS FOR SUSTAINABLE SMART WATER SUPPLY USING DATA PERCEPTION, INTERNATIONAL JOURNAL OF HEALTH SCIENCES ISSN 2550-6978 E-ISSN 2550-696X © 2022, HTTPS://DOI.ORG/10.53730/IJHS.V6NS5.9826, 18 JUNE 2022
[11] SRILATHA PULI, URBAN STREET CLEANLINESS, JOURNAL OF ALGEBRAIC STATISTICS VOLUME 13, NO. 3, 2022, P. 547-552, HTTPS://PUBLISHOA.COM, ISSN: 1309-3452
[12] SRILATHA PULI, SELF-ANNIHILATION IDEATION DETECTION, NEUROQUANTOLOGY | JUNE 2022 | VOLUME 20 | ISSUE 6 | PAGE 7229-7239 | DOI: 10.14704/NQ.2022.20.6.NQ22727
[13] SRILATHA PULI, CRIME ANALYSIS USING MACHINE LEARNING, YMER|| ISSN: 0044-0477, APRIL 2022
[14] SRILATHA PULI, N-GRAMS ASSISTED YOUTUBE SPAM COMMENT DETECTION, YMER || ISSN: 0044-0477, APRIL 2022
[15] SRILATHA PULI, ANALYSIS OF BRAND POPULARITY USING BIG DATA AND TWITTER, YMER|| ISSN: 0044-0477, APRIL 2022
[16] SRILATHA PULI, CYBER THREAT DETECTION BASED ON ARTIFICIAL NEURAL NETWORKS USING EVENT PROFILES,THE INTERNATIONAL JOURNAL OF ANALYTICAL AND EXPERIMENTAL MODAL ANALYSIS, ISSN NO:0886-9367
[17] SRILATHA PULI, FACE MASK MONITORING SYSTEM, THE INTERNATIONAL JOURNAL OF ANALYTICAL AND EXPERIMENTAL MODAL ANALYSIS, ISSN NO:0886-9367
[18] SRILATHA PULI, IOT BASED SMART DOOR LOCK SURVEILLANCE SYSTEM USING SECURITY SENSORS, ADVANCED SCIENCE LETTERS E-ISSN:1936-7317
[19] SRILATHA PULI, SAFETY ALERTING SYSTEM FOR DROWSY DRIVER, 9TH INTERNATIONAL CONFERENCE ON INNOVATIONS IN ELECTRONICS & COMMUNICATION ENGINEERING (ICIECE-2021), PAGE – 40
[20] N. SWAPNA SUHASINI, SRILATHA PULI, BIG DATA ANALYTICS FOR MALWARE DETECTION IN A VIRTUALIZED FRAMEWORK, JOURNAL OF CRITICAL REVIEWS, ISSN:2394-5125 VOL.7, ISSUE 14, JULY – 2020
[21] SRILATHA PULI, BLOCK CHAIN BASED CERTIFICATE VALIDATION, INTERNATIONAL JOURNAL OF SCIENCE AND RESEARCH (IJSR), ISSN: 2319-7064 SJIF (2022): 7.942, VOLUME 11 ISSUE 12, DECEMBER 2022, PAPER ID: SR221219113003, DOI: 10.21275/SR221219113003, WWW.IJSR.NET
[22] MRS. SRILATHA PULI, ENERGY EFFICIENT TEACHING-LEARNING-BASED OPTIMIZATION FOR THE DISCRETE ROUTING PROBLEM IN WIRELESS SENSOR

NETWORK, INTERNATIONAL JOURNAL OF EARLY CHILDHOOD SPECIAL EDUCATION (INT-JECS) DOI: 10.48047/INTJECSE/V14I7.296 ISSN: 1308-5581 VOL 14, ISSUE 07 2022.

[23] MRS. SRILATHA PULI, A HYBRID BLOCK CHAIN-BASED IDENTITY AUTHENTICATION SCHEME FOR MULTI- WSN, INTERNATIONAL JOURNAL OF EARLY CHILDHOOD SPECIAL EDUCATION (INT-JECS) DOI: 10.48047/INTJECSE/V14I7.296 ISSN: 1308-5581 VOL 14, ISSUE 07 2022

[24] MRS. SRILATHA PULI, IMPLEMENTATION OF A SECURED WATERMARKING MECHANISM BASED ON CRYPTOGRAPHY AND BIT PAIRS MATCHING, INTERNATIONAL JOURNAL OF EARLY CHILDHOOD SPECIAL EDUCATION (INT-JECS) DOI: 10.48047/INTJECSE/V14I7.296 ISSN: 1308-5581 VOL 14, ISSUE 07 2022

[25] MRS. S.SUNITHA, MRS. SRILATHA PULI, MULTILEVEL DATA CONCEALING TECHNIQUE USING STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY, INTERNATIONAL JOURNAL OF EARLY CHILDHOOD SPECIAL EDUCATION (INT-JECSE) DOI:10.48047/INTJECSE/V15I1.1 ISSN: 1308-5581 VOL 15, ISSUE 01 2023

[26] MRS. SRILATHA PULI, BLOOD BANK MANAGEMENT DONATION AND AUTOMATION, SPECIALUSIS UGDYMAS / SPECIAL EDUCATION 2022 1 (43), HTTPS://WWW.SUMC.LT/INDEX.PHP/SE/ARTICLE/VIEW/1995

[27] N. S. SUHASINI AND S. PULI, "BIG DATA ANALYTICS IN CLOUD COMPUTING," 2021 SIXTH INTERNATIONAL CONFERENCE ON IMAGE INFORMATION PROCESSING (ICIIP), SHIMLA, INDIA, 2021, PP. 320-325, DOI: 10.1109/ICIIP53038.2021.9702705.

[28] MRS. SRILATHA PULI, KEY-AGGREGATE PROXY RE-ENCRYPTION WITH DYNAMIC CONDITION GENERATION USING MULTILINEAR MAP, JOURNAL OF SURVEY IN FISHERIES SCIENCES 10(1) 2023, PAGES - 2679-2685, E-ISSN: 2368-7487.

[29] MRS. SRILATHA PULI, MRS. SUNITHA SURARAPU, DEEP LEARNING-BASED FRAMEWORK FOR ROBUST TRAFFIC SIGN DETECTION UNDER CHALLENGING WEATHER CONDITIONS, JOURNAL OF SURVEY IN FISHERIES SCIENCES 10(1) 2023, PAGES – 2650-2657, E-ISSN: 2368-7487.

[30] MRS. SRILATHA PULI, MRS. SUNITHA SURARAPU, LICENSE PLATE IMAGE ANALYSIS EMPOWERED BY GENERATIVE ADVERSARIAL NEURAL NETWORKS (GANS), JOURNAL OF SURVEY IN FISHERIES SCIENCES 10(1) 2023, PAGES – 2693-2698, E-ISSN: 2368-7487.

[31] MRS. SRILATHA PULI, MRS. SUNITHA SURARAPU, FOOD CALORIE ESTIMATION USING CONVOLUTIONAL NEURAL NETWORK, JOURNAL OF SURVEY IN FISHERIES SCIENCES 10(1) 2023, PAGES – 2665-2671, E-ISSN: 2368-7487.

[32] MRS. SUNITHA SURARAPU, MRS. SRILATHA PULI, AN INTEGRATED ARCHITECTURE FOR MAINTAINING SECURITY IN CLOUD COMPUTING BASED ON BLOCKCHAIN, JOURNAL OF SURVEY IN FISHERIES SCIENCES 10(1) 2023, PAGES – 2608-2616, E-ISSN: 2368-7487.

[33] MRS. SUNITHA SURARAPU, MRS. SRILATHA PULI, TWO LEVEL LSTM FOR SENTIMENT ANALYSIS USING LEXICON EMBEDDING AND POLAR FLIPPING, JOURNAL OF SURVEY IN FISHERIES SCIENCES 10(1) 2023, PAGES – 2750-2756, E-ISSN: 2368-7487.

[34] MRS. SUNITHA SURARAPU, MRS. SRILATHA PULI, TASK FAILURE PREDICTION IN CLOUD DATA CENTERS USING DEEP LEARNING, JOURNAL OF SURVEY IN FISHERIES SCIENCES 10(1) 2023, PAGES – 2742-2749, E-ISSN: 2368-7487.