International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *30 August 2023* ***Revised:*** *18 October 2023* ***Accepted:*** *02 November 2023*

Enhanced Cauchy Matrix Reed-Solomon Codes and Role-Based Cryptographic Data Access for Data Recovery and Security in Cloud Environment

Vijay R.Sonawane[1], Chetan S. Arage[2], Jaya R.Suryawanshi[3], Santosh P.Jadhav[4], Yogesh H.Palve[5], Mahesh B.Gunjal[6]
[1]MVPS's K.B.T.College of Engineering, Nashik, Maharashtra, India
[2]Sanjay Ghodawat University, Kolhapur, Maharashtra, India
[3]MVPS's K.B.T.College of Engineering, Nashik, Maharashtra, India
[4]MVPS's K.B.T.College of Engineering, Nashik, Maharashtra, India
[5]MVPS's K.B.T.College of Engineering, Nashik, Maharashtra, India
[6] Amrutvahini College of Engineering, Sangamner, Maharashtra, India
[1]vijaysonawane11@gmail.com, [2]chetan.arage@gmail.com,[3]suryavanshi.jaya@kbtcoe.org,
[4]spjadhav375@gmail.com, [5]palve.yogesh@kbtcoe.org [6]maheshgunjal2010@gmail.com

Abstract— In computer systems ensuring proper authorization is a significant challenge, particularly with the rise of open systems and dispersed platforms like the cloud. Role-Based Access Control (RBAC) has been widely adopted in cloud server applications due to its popularity and versatility. When granting authorization access to data stored in the cloud for collecting evidence against offenders, computer forensic investigations play a crucial role. As cloud service providers may not always be reliable, data confidentiality should be ensured within the system. Additionally, a proper revocation procedure is essential for managing users whose credentials have expired. With the increasing scale and distribution of storage systems, component failures have become more common, making fault tolerance a critical concern. In response to this, a secure data-sharing system has been developed, enabling secure key distribution and data sharing for dynamic groups using role-based access control and AES encryption technology. Data recovery involves storing duplicate data to withstand a certain level of data loss. To secure data across distributed systems, the erasure code method is employed. Erasure coding techniques, such as Reed-Solomon codes, have the potential to significantly reduce data storage costs while maintaining resilience against disk failures. In light of this, there is a growing interest from academia and the corporate world in developing innovative coding techniques for cloud storage systems. The research goal is to create a new coding scheme that enhances the efficiency of Reed-Solomon coding using the sophisticated Cauchy matrix to achieve fault tolerance

Keywords- Role Based Access Control, AES, Cloud data security, Multi Authority Access Control, Forensic Investigation, Proxy Key, Cauchy matrix, Reed-Solomon codes, data recovery, Revocable-Storage.

I. INTRODUCTION

In the contemporary era, the primary source of "big data" generation is social networking sites, resulting in vast and complex data sets. The use of mobile devices and the internet has been on the rise, leading to a significant global data proliferation. Consequently, numerous companies are generating massive amounts of data, reaching Petabyte or Exabyte levels. However, traditional systems face limitations in effectively collecting, storing, and analyzing such extensive data, as highlighted by Wang et al. [1].

To safeguard the confidentiality of data stored in the cloud, restricting access is a commonly employed strategy. Over the years, various access control techniques have been proposed in the literature. Among these, Role-Based Access Control (RBAC) stands out as a popular model, especially in managing security for large-scale systems. RBAC associates users with specific roles, which, in turn, have predefined resource rights. Instead of assigning permissions directly to individuals, access is granted based on membership in roles. This approach provides users with adjustable restrictions on data access. RBAC has been actively utilized in numerous systems since its inception in the 1990s [1], and it has undergone refinement and expansion, leading to the suggestion of the RBAC standard in 2000 [3] and further modifications in 1996 [2]. In cloud storage, maintaining data integrity is of paramount importance. Our proposed work aims to safeguard data and enable recovery in case of improper treatment or unauthorized access. A proxy server will be responsible for executing this operation. Both the public and private segments of the cloud storage will hold users' information. Users will be confined to the public cloud to maintain the higher level of security in the private cloud. If any unauthorized alterations occur, the proxy server will restore the original data stored in the private cloud. To achieve an optimal balance between fault tolerance and speed, cloud storage users are offered various redundancy configuration options. In

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *30 August 2023* ***Revised:*** *18 October 2023* ***Accepted:*** *02 November 2023*

distributed storage systems, data accessibility is critical, especially in real-world scenarios where node failures are common. This study investigates secure information storage and exchange using Role-Based Access Control (RBAC), a cloud snapshot-based mechanism for forensic investigation, and the suggested AES 128 encryption technique. A backup server mechanism has been developed to enable ad hoc retrieval for all users, utilizing the server as a proxy storage server. Various existing methodologies were analyzed for potential gaps in knowledge before embarking on the suggested system. Challenges in current computer systems include the time, space, and complexity required to construct matrices. Advancements in processing and storage capabilities have enabled the storage, assembly, and analysis of large datasets. Big data analytics offers novel methods for analyzing vast amounts of data, with applications in fields such as medicine, banking, traffic control, education, and shopping [4]. As data grows, it becomes crucial to address various challenges, including privacy, data integrity, and access control, to protect against potential attacks like data degradation and man-in-the-middle attacks. In this study, models have been developed to manage data recovery for distributed datasets using a Cauchy matrix generating technique.

1.1 Cloud Computing

Cloud computing is a relatively new technology that is still in its early adoption phase. It is described as a network-based solution that provides affordable, dependable, and convenient access to IT resources. While there are various definitions of cloud computing, they all emphasize its service-oriented nature rather than being solely focused on applications. This service-oriented approach not only reduces infrastructure and ownership costs but also grants users more flexibility and improved efficiency [15, 16]. However, the storage of data in the cloud raises significant concerns regarding privacy and security [17]. Ensuring data confidentiality, integrity, and security is crucial for cloud providers [17]. Different service suppliers employ various policies and mechanisms tailored to the type and scale of data to achieve this goal. Cloud computing offers the advantage of data sharing among multiple organizations [15, 16], but this also poses a potential risk to data. Protecting data sources becomes imperative to prevent any potential threats.

Certain information might be too sensitive to be stored in a public cloud, especially data related to national security or highly confidential information about future products. Exposing such data on a publicly accessible cloud could have severe consequences, as it could compromise privacy and accessibility. In such cases, it is advisable to archive the data using the organization's internal cloud. Implementing an on-premises data utilization policy can help enhance data security, but it may not provide complete confidentiality and security for the information, as some organizations lack the expertise to apply all necessary layers of security to private data [17].

1.2 Data Security in Cloud Computing

Data encryption represents just one aspect of cloud computing's comprehensive approach to safeguarding data. The three distinct service models—SaaS, PaaS, and IaaS—impose varying data protection requirements [18]. Data is stored "at rest" when residing in the cloud, and "in transit" when flowing to and from the cloud, both forms carrying potential privacy risks (see figure 1.1). The level of data privacy and security is determined by the characteristics of data security procedures, processes, and systems. Addressing data vulnerability in each of these states is of utmost importance.

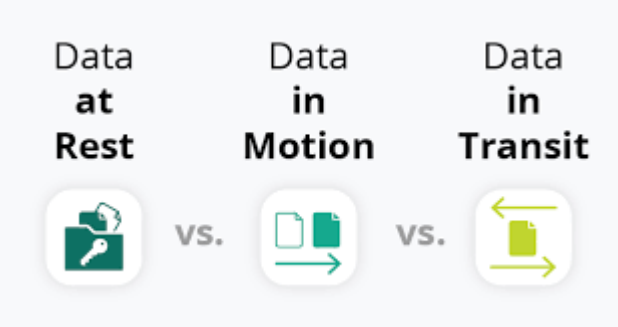

Figure 1.1: Data at Rest and in Transit

Yang et al. [5] propose a multi-cloud computing storage solution that prioritizes privacy and cost efficiency. Chervyakov et al. [6] suggest a distributed data storage system for processing encrypted data and managing computation, while errors are identified and corrected using the Duplicate Atomic Number System. Research on blockchain security architecture for distributed cloud storage is also ongoing. Li et al. [7] explore a genetic algorithm to address file block replication among users and data centers, and Bhuvaneshwari & Tharini [8] emphasize the need for scalable and reliable distributed storage systems due to the growing volume of data. Furthermore, Low-Density Parity Check (LDPC) algorithms are under investigation for large-scale data storage. Tang & Zhang [9] present a method for simplifying the design of encoders and decoders using a Vandermonde matrix concatenated with an identity matrix.

Numerous investigations have explored finite field theories to reduce one-in-bit matrices of the Cauchy matrix. Cauchy Reed-Solomon (RS) codes are known for their resistance to erasures. Makovenko et al. [10] describe the use of heuristic modification to enhance coding bit-matrices for fault-tolerant data storage. One of the crucial criteria for cloud storage solutions is their ability to serve multiple customers simultaneously, and this is now represented by a new region called the help rate. Kazemi et al. [11] propose a Quality of

Service (QoS) metric for programmed, distributed settings to handle multiple information access requests concurrently.

Chen & Ma [12] present an effective and cost-efficient disc recovery technique that reduces the amount of data read from the disc. It ensures a consistent burden across all surviving discs, requiring only a small number of disc reads to restore the failed disc. However, recovering all the data can be time-consuming. Shen et al. [13] demonstrate how to calculate the ideal number of code word images for XOR-based erasure codes. Their approach minimizes the amount of information needed to build recapture rosters and enhances I/O efficiency for cloud document frameworks with large square dimensions, reducing the volume of material read during recovery. The only drawback is that it requires a substantial portion of resources. The research study introduces the Advanced Cauchy Reed Solomon (ACRS) approach as a complementary method to the "Reed Solomon" technique. By utilizing the XOR technique, which eliminates the need for Galois Field Multiplication, ACRS streamlines the encoding process and ensures efficient erasure maintenance and data recovery after loss. This ACRS code converts "k" data blocks into "m" coding blocks, effectively managing "m" disc failures using the new approach. In the context of cloud computing, the sharing of various resources, such as software, hardware, and processing units, is explored. The service offered is highly cost-effective and scalable [14]. Cloud computing has garnered significant interest from both business owners and cybercriminals due to its attractive features. To gather evidence against criminals, "computer forensic investigation" becomes crucial. However, modern technology and cloud computing techniques pose challenges for forensic investigation procedures. Key obstacles include dealing with conflicting rules for data stored in different locations, limited access to cloud-based evidence, and the difficulty of seizing physical evidence to establish integrity or present evidence.

In the contemporary realm of cloud computing, the speed at which new information is generated and stored in the cloud has accelerated compared to previous periods. As a result, cloud storage has emerged as a crucial element within cloud computing [86]. Nowadays, cloud computing is widely used for data storage due to its desirable features, including broad network access, resource pooling, on-demand availability, and managed services. However, the risk of potential data loss exists in case of unfavorable events like power surges, broken drives, hardware failures, or coding errors within the system.. Therefore, maintaining the integrity of data should be the central focus of cloud storage. This entails employing measures, including the TTP protocol, to safeguard the data and implement procedures to recover it in case of mishandling. A Proxy server is tasked with completing the given assignment. Client information is stored in both the public and private sections of the cloud storage. Access to data stored in the public cloud is granted to users, while the private cloud maintains a higher level of security. The Proxy server promptly retrieves the original information from the private cloud if any unauthorized changes occur and returns it to the user. Cloud storage users are typically provided with various redundancy configuration options, aiming for optimal efficiency and an acceptable level of fault tolerance. In distributed storage networks, data accessibility is crucial, especially when node malfunctions are common. This research explores secure data transmission and storage using AES 128 encryption and Role-Based Access Control. Additionally, a backup server method is employed in this study, acting as a proxy storage server and enabling ad hoc data recovery across all dispersed data servers. The data storage system provided in the cloud should ensure the protection of the user's files. This can be achieved by replicating the data, which means keeping multiple copies in different locations. While replication is simple and allows some level of information loss tolerance, it is not very storage-efficient. To improve both security and storage efficiency, erasure codes are gradually replacing duplication in cloud system files. Erasure coding, such as reed-solomon codes, is a method used in distributed systems to safeguard data. It has shown promise in significantly reducing data storage costs while maintaining the same level of fault tolerance against disk malfunctions. However, it is worth noting that erasure coding has some drawbacks, including higher costs for repair and longer access latency. As a result, there is a growing interest in academia and the corporate world to develop new coding methods for cloud-based data storage. The proposed research aims to enhance the effectiveness of the reed-solomon coding technique by introducing a novel coding strategy that utilizes the Enhanced Cauchy Matrix. This approach is expected to provide improved fault tolerance while addressing some of the limitations associated with traditional erasure coding methods.

II. LITERATURE SURVEY

Yong Wang, designed and implemented an RBAC framework that relied on data encryption to ensure secure access control [19]. They employed attribute-based encryption in a two-step user job process and a job assent activity method, achieving two main objectives: maintaining reliable access techniques and reducing dependency on specific decision centers for access decisions. Their approach involves attribute-based user job classifications and role authorization allocations, making the access control process more flexible and adaptable. Additionally, they integrated their methods into an RBAC prototype. The successful testing of this prototype and the recognition of its support demonstrate the potential feasibility of their concept. Considering the security objectives is essential in building a trustworthy and dependable trust-based system.

Mahdi Ghafoorian introduced a new approach to Role-Based Access Control (RBAC) that centers around trust and credibility [20]. This novel RBAC paradigm not only effectively addresses security threats associated with trust-based RBAC systems but also demonstrates adaptability with reasonable implementation time.To evaluate their proposed model, the researchers utilized the well-established trust framework found in the Advogato dataset. The results of the evaluation showed that the suggested prototype differed from existing models in terms of error rates, implementation time for sophisticated trust calculations, and the incorporated characteristics. Notably, the suggested prototype incorporates specific features, making it stand out from previously circulated types.The findings from the evaluation indicate that the proposed RBAC model is well-suited for deployment in cloud environments, as it has been successfully validated under such conditions.

Gadouche et al. [21] recommend using the Event-B approach for implementing a customized attribute-based access control (ABAC) system. To systematically build a suitable prototype, they rely on the previous verifications they have obtained. The prototype demonstrates different levels of evaluation achieved by fulfilling responsibilities in the refining process. Various aspects of ABAC are discussed at each refinement level, starting from the most advanced and unique level and progressing to the most fundamental one. These characteristics are documented within the proofs themselves, specifically in the behavior particulars. The process can be accessed on the websites of the organizations responsible for administering social insurance.

Muthunagai et al. [22], it is challenging to securely store customer information on a personal storage system located close to the business. To address this issue, the researchers propose using cloud storage, which allows the user's data to be stored in a remote database. This way, users can access their documents from the cloud storage platform, regardless of the physical location of the data. To ensure privacy, the research employs a method that involves splitting and encrypting the user's data using an improved attribute-based encryption technique. The data is repeatedly encrypted until all the fragments are secure. These encrypted data pieces are then distributed across multiple locations to protect the client's supplied data from unauthorized access by third parties. To retrieve the data stored in a specific location efficiently, a decoding technique is employed, reducing system congestion during the retrieval process. This is particularly beneficial when retrieving data from an independent site. The combined approach of data splitting, encryption, distributed storage, and decoding contributes to enhanced data security and efficient data retrieval for cloud-based storage systems.

Viswanath et al. [23] devised a technique that enables the secure uploading of information or data into a cloud-based architecture. Prior to uploading, this method encrypts the data, ensuring its confidentiality. The cloud storage service contains the simulation results and a total of 2630 KB of encrypted data. The algorithm's effectiveness was assessed using real-time health information gathering, resulting in a more precise evaluation of its capabilities. Li, H. et al. [24] developed an innovative approach to image compression for compressed sensing, which includes an encryption process for safeguarding photographic image confidentiality. They employed a stochastic method to achieve this encryption. Bale et al. [25] conducted an investigation into various techniques like AES, BRA, RC4, and Blowfish for ensuring secure blockwise operations. These methods fall under symmetric cryptography, implying the use of the same key for both encoding and decoding information. Their proposed multithreading procedure contributed to achieving low latency. Compared to AES, their method exhibited around 20% faster text file encoding times.

I. T. Singh et al. [26] conducted research focusing on evaluating the Round Robin technique in Server Load Balancing (SLB) using Software Defined Networking (SDN). The Round Robin method proved to be highly effective, ensuring 100% server availability, as demonstrated in the experiment outcomes. Load balancing among live servers in the server pool was achieved through this method. The experimentation employed a POX controller and an OpenFlow switch to implement the Round Robin load-balancing approach. In their work, X. Yu et al. [27] developed and assessed Vandermonde and Cauchy MDS array codes for their encoding and decoding efficiency. The test results revealed that Vandermonde MDS array codes outperformed Cauchy MDS array codes in terms of both encoding and decoding capabilities. Specifically, the encoding rate of Vandermonde MDS array codes was approximately 58% better than that of Cauchy MDS array codes, and the decoding rate of Vandermonde MDS array codes was approximately 70% higher than that of Cauchy MDS array codes. The proposed system relied on the LU factorization of Vandermonde and Cauchy matrices for an effective decoding approach. However, this study only covered some aspects of the decoding technique of Vandermonde MDS array codes.

L. Bannawat et al. [28] propose a method for identifying and categorizing buried improvised explosive devices using ground-penetrating radar (GPR) and the Cauchy method. The GPR system collects signals, which are used to create B-scan images. The Cauchy method facilitates direct extraction of poles from the frequency responses acquired by the GPR system. These extracted poles are then used to categorize buried objects, such as petrol tanks and empty holes. To assess

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *30 August 2023* ***Revised:*** *18 October 2023* ***Accepted:*** *02 November 2023*

the method's effectiveness, the researchers ran simulations using electromagnetic software, considering single and multi-layer interfaces. The results indicate that the proposed strategy, employing the Cauchy technique, is capable of effectively identifying and categorizing buried items based on the retrieved poles.Guangyan Zhang et al. [29] developed an efficient Cauchy coding approach (CaCo) for information storage in the cloud. The method involves using Cauchy matrix heuristics to create a matrix set and then employing XOR schedule heuristics to construct schedules for each matrix in the set. CaCo selects the most compact schedule from the prepared ones, allowing it to determine the most effective coding scheme for any redundancy configuration. The simplicity of CaCo enables easy parallelization, making it efficient when utilizing abundant computational resources available in the cloud. The researchers implemented CaCo in the Hadoop distributed file system and compared its efficiency with "Hadoop-EC" developed by Microsoft research. The experimental results indicate that CaCo achieves an ideal coding scheme in an acceptable timeframe and outperforms Hadoop-EC. S. Ren et al. [30] address the issue of excessive computational complexity in the hardware version of Galois Field (GF) multiplication used in common Reed-Solomon (RS) coding methods. They propose a redesign of a half-multiplier based on the matrix approach and optimize the RS coding component. Simulation results show that the hardware resources required for encoding with the developed encoder are approximately 15% lower than those needed for encoding with the Xilinx official encoding device, while maintaining the same level of coding precision.

Orthogonal Frequency Division Multiplexing (OFDM) is a statistical multi-carrier modulation technique that goes beyond the concept of modifying individual subcarriers, as mentioned in V. R. Ch et al.'s work [31]. Instead of transmitting a high-rate data stream over a single subcarrier, OFDM utilizes multiple subcarriers within a single channel. These subcarriers are distributed in a synchronized manner and are orthogonal to each other. Each subcarrier is modulated at a lower symbol rate than the average, employing a modulation technique.Compared to traditional single-carrier modulation methods operating within the same bandwidth, OFDM, with its combination of multiple subcarriers, achieves much higher information speeds. However, to enhance error correction capacity in OFDM, effective channel coding is crucial. To address this, a channel coding strategy based on Reed Solomon (RS) codes, known for their strong error-correcting capabilities, was chosen.The main objective of this research is to design a channel coding strategy using RS codes to improve the efficiency of OFDM. The proposed approach was tested using the Additive White Gaussian Noise (AWGN) fading channel along with various modulation techniques. The effectiveness of the suggested method, both with and without RS channel coding, was evaluated through Bit Error Rate (BER) analysis, and the results were found to be satisfactory.The simulation outcomes clearly demonstrate that the use of RS channel coding significantly enhances the BER for OFDM, validating the effectiveness of the proposed approach.

By implementing AES encryption algorithms and RBAC, a secure data-sharing platform is being constructed. This system facilitates secure key distribution and enables information sharing among dynamic groups. The data recovery process involves duplicating information to withstand certain levels of data loss. To ensure data safety across all distributed systems, the erasure code technique is employed.Modern erasure coding strategies, like Reed-Solomon codes, offer the potential to significantly reduce the cost of storing information while maintaining the same level of error resistance caused by disk malfunctions [32, 33, 34].However, this approach has drawbacks, including a more pronounced access delay and higher repair expenses. Due to these challenges, there is considerable interest from academia and the business sector in developing innovative coding strategies for cloud-based data storage. This investigation aims to create a new coding method that enhances the performance of the Reed-Solomon coding strategy.

III. THEORY AND FORMULA

This system utilizes the intricate Cauchy matrix to achieve fault tolerance. As a result, the proposed system is designed in two stages: 1**.** AES technique for ensuring data security and role-based access control in the cloud 2**.** Enhanced Cauchy Matrix (ECM) technique employed for data recovery in the cloud environment. The comprehensive explanation of these two phases is provided below.

1.3 A novel approach for securing data in the cloud using AES encryption and role-based access control (RBAC)

With the rapid growth of cloud computing and the increasing popularity of storing vast amounts of information in the cloud, the need to prevent unauthorized access to sensitive data has become a crucial concern. To address this, a secure data sharing strategy has been developed, leveraging RBAC and AES encryption. This approach ensures secure key distribution and enables safe data exchange for dynamic parties.The proposed technology not only protects data but also allows for its regeneration in case it is mishandled by unauthorized users. To achieve this, a Proxy server is assigned the responsibility of managing access control. Data pertinent to users can be stored in either the public or private areas of the cloud storage, ensuring a robust and secure system. Users will be restricted to accessing only the data stored in the public cloud to ensure the heightened security of the private cloud remains intact. If any unauthorized changes are detected in the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *30 August 2023* ***Revised:*** *18 October 2023* ***Accepted:*** *02 November 2023*

data, a proxy server promptly grants users access to the original information stored in the private cloud. Cloud storage users are typically offered various redundancy settings, allowing them to optimize performance while maintaining an acceptable level of fault tolerance. The system can achieve both the highest level of security and maximum privacy concurrently. The proposed AES approach for Role-Based Access Control (RBAC) is designed to enable secure data sharing in untrusted environments, such as cloud computing. The Trusted Proxy Authority (TPA) plays a crucial role in facilitating and ensuring secure interactions among various parties. In this system, users can obtain both their master and private keys securely from the intermediary authority. Additionally, the system offers a reliable mechanism for secure revocation, even for users who are not trustworthy. To enhance security further, the research proposes the generation of proxy keys as a potential future improvement. When a data holder revokes access for a specific end user, the system promptly invalidates all active keys and generates fresh keys for each shared user. This approach guarantees the highest level of security and privacy concurrently. Distributed data access control is a dynamic mechanism enabling efficient attribute revocation in multi-authority cloud storage platforms. Unlike centralized systems, it allows modifications at any point in time. By relieving users from the burden of decryption based on attributes, this robust attribute-based encryption technology ensures the constant security of sensitive information in cloud storage. Such an approach holds promise in various scenarios, ranging from online social networks to off-site storage facilities, offering a versatile and beneficial solution for safeguarding data.

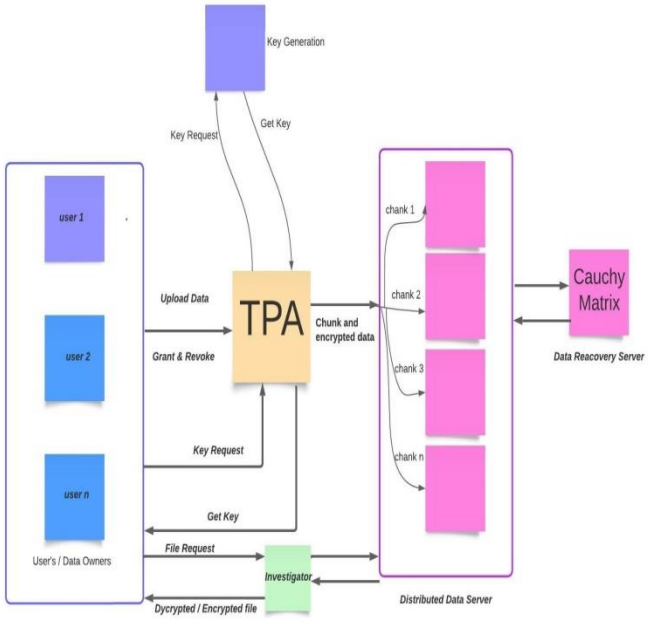

Figure. 3.1 Proposed System

Figure 3.1 illustrates the matrix-based architecture used for managing and evaluating the cloud data structure. The framework incorporates components required for a managerial broadcast network and provides a node controller for the domain. Data packets are transferred from endpoints to data sources at scheduled intervals or when specific activities are planned.The CaCo layout also includes an additional self-address calibrating component to facilitate data decoding and address retrieval, expediting the process. The proposed alternative prioritizes reducing wait times and enhancing system effectiveness. The algorithm initially calculates values for (k, m, w), where k represents the total number of chunks, M represents the matrix nodes, and w is the sum of k and m. This calculation occurs at the process's outset.Once the k, m, and w vectors are fully adhered to, the document can be uploaded. When k, m, and w are 4, 2, and 6 respectively, the framework generates four chunks to store encrypted information, utilizing data nodes. To save the data, an [8 * 8] matrix is produced for each method. Each data chunk is stored on a data node, and the matrix is switched into master mode. In case of system breakdown, the matrix and any remaining data nodes can retrieve the data.

3.2.1 Algorithm

The steps of Equally Load Re-Balancer algorithm and Load Balancer Algorithm are discussed as follows:

3.2.1.1 Equally Load Re-Balancer Algorithm

Input : The load of every node is based on the current hitting.
Output: Data transmitted to every node in the network.
Steps: 1. Set the value of n for each of the data nodes that are connected to the master node.
2. for each iteration (j to n), Determine the load on the jth node server.A[j] denotes the degree of load on the ith node, also known as the hitting load.
3. determine the overall length of A. produce the data chunks that were required. M=A.length();
4. Construct k mappers for propagate a data.
5. Give each chunk to one of the mappers in turn.
6. Requesting server for storing a data.
7. The procedure is finished.

3.2.2.2 Load Balancer Algorithm

Input: data-containing text files
Output: Processing of files with load balancing on the server
Steps:
1. Start the main server and all of its subordinate servers.
2. Using either the Internet Protocol address or the port number, create a link among the sub-server along with the servers.
3. Transfer the file to the server so that it can be shared.
4. The data on the server are encrypted using AES Encryption.
5. Divide the file into several separate portions.
6. Determine how much memory all of the sub servers has.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *30 August 2023* ***Revised:*** *18 October 2023* ***Accepted:*** *02 November 2023*

7. Partition the total sum of the chunks by the entire amount of servers in the cluster.
8. Transfer every chunk into sub servers according to the amount of memory that it has.
9. If the amount of space is lower than expected, then move any excess chunks to one of the subsequent sub-servers.
10. An index value will get added to every chunk that is taken in.
11. Whenever a client requests a file, the request for it will be fulfilled by one of several sub-servers, the selection of which is determined by the index value.
12. The client is responsible for gathering each of the chunks, after which the document will be encrypted and the user will be able to view it.

3.3 Proposed Enhanced Cauchy Matrix (ECM) technique for data recovery in cloud Environment

3.3.1 Enhanced Cauchy Reed-Solomon Coding

The Reed-Solomon (RS) coding system is a technique based on a finite area known as a Galois field. However, it requires numerous computations, like additions and multiplications, which can limit its effectiveness in data encryption. To address this, an evolution of RS codes called Cauchy Reed-Solomon (CRS) codes [35] was introduced, bringing two improvements. Firstly, instead of using Vandermonde matrices, CRS codes utilize Cauchy matrices as a more efficient alternative in the encoding process. Secondly, the Galois field multipliers needed for CRS codes are replaced with XOR calculations, further optimizing the encoding procedure. The ECM method proposes a data recovery technique based on regenerating codes. In the research, an Effective Cauchy Matrix is proposed to generate matrices through matrix heuristics. This enhanced Cauchy matrix can be employed in Reed-Solomon codes to serve as generating matrices for encoding data chunks while reducing the number of XOR operations required. This improvement is made possible by the ECM method. When attempting to recover data from damaged discs using the Reed-Solomon method, the technique requires three parameters: redundancy configuration, parity, and data block. Only with these parameters, the program can effectively retrieve the data. The recently proposed ECM approach relies on the RS code as its foundation. ECM model operates to recover data in the cloud. In this scenario, encoding and decoding are distinct procedures that necessitate cooperation among various parties. The entities involved in the coding process include the client, data files, server nodes, as well as the data and parity blocks. ECM strategy, when a client wants to write specific information to a file, the first step involves directing their request through the encoding block. This block serves as the location where documents from the client are written onto the server terminals. This marks the initial phase of the process when a client wishes to store data in a file.

As part of the encoding method, the client's original data file intended for the server's node undergoes a transformation into a different format to protect the data and prevent unauthorized access. This encoding process aims to increase system reliability and data accessibility in case of disk failures. The file obtained from the client is encrypted during the encoding procedure. During encoding, the ECM technique incorporates redundancy configurations (l, m, n) to create the validation matrix. In this specific system, the character 'n' represents the number of coding unit bits per word, 'm' indicates the number of parity blocks, and 'l' stands for the number of data blocks. The current study explores the trade-off between the time required to construct a matrix and the resources utilized. The duration for matrix creation is compared to the overall resource consumption within a distributed environment. To accomplish this, a mathematical model of the system is established, employing XOR operations to generate each Cauchy coding matrix for individual components. The construction of Cauchy matrices on GF (Galois Field) is also utilized, offering the additional benefit of reducing the total number of GF additions and multiplications.

3.3.2 ECM encoding Algorithm

The Enhanced Cauchy matrix and the data blocks that are used in the data write process can both be encoded using the step-by-step process that has been given in Algorithm 1.

Algorithm 1:

ECM encoding algorithm

Input: {*l*,*m*,*n*}

Wherein l, m, n indicates data blocks, parity blocks and coding units bits for each word

Output: Code word check matrix

The proposed EMC method for the recovery of data transforms the Cauchy encoding elements into Boolean format and stores the result as a binary matrix. After that, additional binary XOR computations are carried out on the components that were derived from the Galois Field GsF(2^n). Computations involving XOR can be made more efficient as a result, saving time and effort. In this phase of the encoding procedure, there are three factors that are taken into consideration when designing the Cauchy matrix. These variables are l, m, and n, where l represents the total number of data blocks, m represents the quantity of parity blocks, and n represents the number of coding unit bits each word.

3.3.3 Data Recovery Algorithm

The write procedure that is carried out by utilizing the Ca-Co technique for the purpose of data storage in a cloud-based setting is outlined by Algorithm 2.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 30 August 2023 **Revised:** 18 October 2023 **Accepted:** 02 November 2023*

Input: Code word check matrix

Output: Clear text

Step 1: User send an extraction of data request to server end.

Step 2: Decoding matrix construction.

As *Res1* is divided into the data blocks of $(p+l) \times q$ and matrix *BMx(d)* which consists $(p+l)\ q \times (p+l)\ w$ in dimension *is* developed.

$$BMx(d) = \frac{(Identity\ matrix | matrix\ zero)}{(Parity\ matrix\ of\ Res1)}$$

Step 3: Determine the data blocks that are lacking.

(a) The data of the entire section is lost whenever a data node experiences a failure. As a result, a related list L of elements that are missing is compiled for the node that is absent while the data is being re-established.

(b) An iteration is performed on the component that is not present d in the list L of the elements that are missing. Assuming that it is relevant to the data element, go to step c. If it fits in with the unnecessary component in any way, disregard it.

(c) The row set r is the one in the parity check matrix H in which the element d has the value 1. Assuming that r does not include any components, make row d equal to zero. If there is an element lacking from r, then choose the row with the smallest weight of Hamming and label it r1. This is done in the event that there is an element in r. The row that corresponds to the element in r and the row that corresponds to d both conduct an XOR operation with r1, and r1 has been set to 0.

(d) Once all of the elements of list L have been responded to, the values in the column that corresponds to the superfluous elements of the list can have their values reset to zero.

IV. RESULT DISCUSSIONS

Cloud computing, a revolutionary technology, has become highly beneficial in our modern daily lives. It utilizes the internet and centralized remote servers to provide and maintain applications and data. Users can conveniently access these programs through cloud-based communication, eliminating the need for manual installations. Furthermore, users' data files can be accessed and modified from any device thanks to internet-based services.

Despite the flexibility cloud computing offers in accessing and utilizing applications and data, concerns persist about ensuring a secure environment that protects information and applications from unauthorized access and breaches [15,16,17]. In response to these security challenges, the proposed research approach takes into consideration various security flaws and employs both AES encryption and role-based access control methods to enhance data protection and prevent potential breaches. Cloud computing systems provide users with a broad range of user-friendly computing and data storage options [18]. The process of transferring data to the cloud is straightforward. The cloud's main server stores a vast amount of personal data generated by the cloud computing system. As the demand for information retrieval services increases daily, effective data recovery strategies are being researched and developed [36,37]. The data recovery method's purpose is to retrieve information from the backup server in case the primary server experiences data loss and cannot provide the user with the required data. The study focuses on the data recovery approach that utilizes the Enhanced Cauchy Matrix.

The investigation was conducted on a group of three devices, each equipped with an Hp Q6600 2.40 GHz quad-core CPU, 4 gigabytes of RAM, and two 7200 RPM hard disks. These machines formed a cluster and were connected using gigabit switched Ethernet. The purpose of the experiments was to determine the length of the cipher text.

The RBE scheme overview revealed that the cipher texts do not contain any user-related information. Instead, they are generated using parameters that hold the individual identities for each ancestral duty associated with the target role. Therefore, the ciphertexts do not include any user-specific details.

To exemplify this concept, we compare a situation where the intended role has 10, 100, and 1000 ancestor duties, respectively. Based on this comparison, we determine the dimensions of the cipher text, which are outlined in Table 4.1. Meanwhile, the plaintext sizes were 1000, 10000, and 100000 byte values, respectively. Initially, it was observed that the disparities in size between the plaintext and the cipher text remain consistent. This observation is made as a preliminary step before proceeding to the next stage.

Furthermore, it has been established that the overall dimension of the cipher text remains unchanged, regardless of the number of ancestor jobs implemented in the algorithm. The length of the cipher text maintains a direct proportional ratio to the length of the plaintext, regardless of the number of authorized roles or clients decrypting the cipher text.

TABLE I. LENGTH OF THE CIPHERTEXT IN BYTES

Length of the Plaintext	10 Tasks	100 Tasks	1000 Tasks
1000	1432	1432	1432
10000	10432	10432	10432
100000	100432	100432	100432

The size of the decryption key is a crucial aspect of the cloud-hosted storage system. According to the study results,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 30 August 2023 **Revised:** 18 October 2023 **Accepted:** 02 November 2023*

the decryption key's total length is 48 bytes, which strikes a balance as it is neither too large nor too small for users' convenience. Users often struggle to determine the memory requirements on their client machines to store encryption keys, especially when decryption keys don't have fixed sizes. This uncertainty makes it difficult for users to ensure their devices can handle encryption keys.

The encryption and decryption processes consume the majority of system time. To optimize decryption, it is split, allowing execution by either the client or the cloud simultaneously. The time required for cloud decryption is measured from the moment ciphertext delivery to the client begins after obtaining the role parameters from the private cloud's server. This approach helps gauge the decryption time. As cloud data decryption demands significant computational power, it is divided into multiple threads. Utilizing multiple cores in the cloud allows parallel processing of these threads, reducing the decryption time. This method effectively minimizes the time needed to decrypt data in the cloud.

In the research framework, the number of active threads is increased to simulate a growing number of processor cores. However, since the computation process relies on only one thread, the quad-core server can only emulate a maximum of 3 cores, as the master thread is the only one that uses more than one thread.

V. EXPERIMENT OF CAUCHY

This passage discusses the different experiments conducted to assess the efficiency of encoding and decoding procedures in a distributed environment concerning the time required for each operation. The evaluation parameters for the system's effectiveness are presented in Table II.

TABLE II. SYSTEM REQUIREMENTS

Particulars	Specifications
CPU with RAM	CPU of a Pentium 2.5 gigahertz and 4 gigabytes of RAM
Cloud computing services	Amazon EC2
Web technologies	HTML, JavaScript

TABLE III. TIME REQUIRED FOR ENCODING AND DECODING DIFFERENT SIZED INPUT FILES FOR THE PROPOSED ECM METHOD (WITH L AND M AS 10, 20 RESPECTIVELY)

File size	Encoding Time	Decoding Time
1 MB	0.12	0.145
5 MB	0.26	0.31
10 MB	0.54	1.3

The total amount of time, in seconds, that is required to code files with sizes ranging from 1 to 10 megabytes can be seen in Table III. This time is required when utilizing the proposed ECM method.

TABLE IV. PERFORMANCE ANALYSIS OF PROPOSED OCC FOR VARIOUS INPUT PAIR VALUES (L, M)

Encoding in term of (l, m)	Availability	Recoverability	Efficacy	Storage Expenses
(4,1)	High	High	High	Low
(5,1)	High	High	Medium	Low
(6, 1)	High	High	High	Low
(7, 1)	High	High	High	Medium
(4, 2)	High	High	High	Low
(4, 3)	High	Medium	High	Low
(4, 4)	High	High	Medium	Low
(4, 5)	High	Medium	Low	High

Table 4 gives the details on the various factors in the scenario that a disc malfunctions to read or write data. This information includes the accessibility of data, recovery, effectiveness, and storage expense. For the given input parameters l=4 and m=1, accordingly, it displays superior levels of data accessibility, high recovery and effectiveness. When compared to other configurations, the storage expense is rather low. When the total quantity of parity blocks that are being used in a system grows, the quantity of storage space that is necessary likewise grows.

The results of an analysis of the mean amount of time needed by various techniques to complete encoding and decoding activities on a data set that is 1024 kilobytes in size are presented in Table 5. The time needed to complete tasks using the proposed system is significantly less than the time needed to complete tasks using either of the two approaches that are presently in use.

TABLE V. TABLE 4.5: MEAN ENCODING AND DECODING TIME OF VARIOUS TECHNIQUES (WITH FILE SIZE, L, M AS 1024KB, 4 AND 10 RESPECTIVELY)

Methods	Encoding Time(s)	Decoding Time(s)
OWSPM-MSR	0.115	0.23
PM-MSR	0.043	0.15
ECM	0.034	0.1159

VI. CONCLUSIONS

A novel method for secure data sharing in the cloud, based on role-based access control, has been proposed. The approach is designed to ensure data security even in an untrusted environment. Through middleware providers, users can securely obtain their master and private keys. The system also facilitates encrypted communication among multiple parties by employing Trusted Proxy Agents (TPAs). Moreover, the technique enables secure revocation for untrusted users. To achieve this, the study suggests generating proxy keys. When a data owner revokes access for a specific end user, the system automatically discards existing keys and generates new ones

for all shared users. These strategies collectively contribute to achieving the highest level of security and privacy.

The development and implementation of innovative coding schemes for cloud data storage have attracted significant interest from various sectors, including corporations and academia. The research aimed to devise a unique coding approach to enhance the efficiency of the Reed-Solomon coding program. To achieve fault tolerance, the proposed approach utilizes the challenging Cauchy matrix.

REFERENCES

[1] J. Wang, Y. Yang, T. Wang, R. S. Sherratt, J. Zhang, "Big Data Service Architecture: A Survey," Journal of Internet Technology, vol. 21, no. 2, pp. 393-405, Mar. 2020.

[2] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, “Role-based access control models,” IEEE Comput., vol. 29, no. 2, pp. 38–47, Feb. 1996.

[3] R. Sandhu, D. Ferraiolo, and D. Kuhn, “The NIST model for role-based access control: Towards a unified standard,” in Proc. RBAC, 2000, pp. 47–63.

[4] N. A. Ghani, S. Hamid, I. A. T. Hashem, E. Ahmed, “Social Media Big Data Analytics: A Survey”, Computers in Human Behavior, Vol. 101, pp. 417-428, 2019, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2018.08.039.

[5] J. Yang, H. Zhu, T. Liu, “Secure and Economical Multi-Cloud Storage Policy with NSGA-II-C”, Applied Soft Computing, Vol. 83, 2019, 105649, ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2019.105649.

[6] N. Chervyakov, M. Babenko, A. Tchernykh, N. Kucherov, V. Miranda Lopez, J. M. Cortes-Mendoza, “AR-RRNS: Configurable Reliable Distributed Data Storage Systems for Internet of Things to Ensure Security”, Future Generation Computer Systems, Vol. 92, 2019, Pages 1080-1092, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.09.061.

[7] J. Li, J. Wu, L. Chen, “Block-secure: Blockchain Based Scheme for Secure P2P Cloud Storage”, Information Sciences, Vol. 465, pp. 219- 231, 2018, ISSN 0020-0255.

[8] P. V. Bhuvaneshwari & C. Tharini, “Review on LDPC Codes for Big Data Storage”, Wireless Personal Communications, Vol. 117, Issue 2, pp. 1601-1625, 2021.

[9] Y. J. Tang and X. Zhang, "Fast En/Decoding of Reed-Solomon Codes for Failure Recovery", IEEE Transactions on Computers, vol. 71, no. 3, pp. 724-735, 1 March 2022, https://doi: 10.1109/TC.2021.3060701.

[10] M. Makovenko, M. Cheng and C. Tian, "Revisiting the Optimization of Cauchy Reed-Solomon Coding Matrix for Fault-Tolerant Data Storage," IEEE Transactions on Computers, https://doi: 10.1109/TC.2021.3110131.

[11] F. Kazemi, S. Kurz, Soljanin and A. Sprintson, “Efficient Storage Schemes for Desired Service Rate Regions”, 2020 IEEE Information Theory Workshop (ITW), pp. 1-21, 2020.

[12] X. Chen and X. Ma, "Optimized Recovery Algorithms for RDP $(p, 3) $ Code," in IEEE Communications Letters, vol. 22, no. 12, pp. 2443-2446, Dec. 2018, https://doi: 10.1109/LCOMM.2018.2875468.

[13]] Z. Shen, J. Shu and P. P. C. Lee, "Reconsidering Single Failure Recovery in Clustered File Systems," 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016, pp. 323-334, doi: 10.1109/DSN.2016.37.

[14] M. Damshenas, A. Dehghantanha, R. Mahmoud and S. bin Shamsuddin, "Forensics investigation challenges in cloud computing environments," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, Malaysia, 2012, pp. 190-194, doi: 10.1109/CyberSec.2012.6246092.

[15] G. S. Puri, R. Tiwary and S. Shukla, "A Review on Cloud Computing," 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2019, pp. 63-68, doi: 10.1109/CONFLUENCE.2019.8776907.

[16] N. Tissir, S. El Kafhali and N. Aboutabit, "Cloud Computing security classifications and taxonomies: a comprehensive study and comparison," 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), Marrakesh, Morocco, 2020, pp. 1-6, doi: 10.1109/CloudTech49835.2020.9365884.

[17] W. Zeng and V. Germanos, "Benefit and Cost of Cloud Computing Security," 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Leicester, UK, 2019, pp. 291-295, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00093.

[18] Ahmed Albugmi, Madini O. Alassafi and Robert Walters, Gary Wills, “Data Security in Cloud Computing”, fifth International Conference on Future Generation Communication Technologies (FGCT 2016)

[19] Y. Wang, Y. Ma, K. Xiang, Z. Liu and M. Li, “A Role-Based Access Control System Using Attribute-Based Encryption,” in IEEE Int. Conf. Big Data Artific. Intellig. (BDAI), June 2018, pp. 128-133.

[20] M. Ghafoorian, D. Abbasinezhad-Mood and H. Shakeri, “A thorough trust and reputation based RBAC model for secure data storage in the cloud,” IEEE Tran. Paral. Distribut. Sys., vol. 30, pp.778-788, 2018.

[21] H. Gadouche, Z. Farah and A. Tari, “A correct-by-construction model for attribute-based access control,” Clust. Comp., pp. 1-12, 2019.

[22] S. U. Muthunagai and R. Anitha, “Secure Access Control Method in Cloud Environment Using Improved Attribute Based Encryption Technique,” Int. J. Engineer. Adv. Tech. (IJEAT), 2019.

[23] Viswanath, G., & Krishna, P. V. (2020). Hybrid encryption framework for securing big data storage in multi-cloud environment. Evolutionary Intelligence, 1-8.

[24] Li, H., Yu, C., & Wang, X. (2020). A novel 1D chaotic system for image encryption, authentication and compression in cloud. Multimedia Tools and Applications, 1-38.

[25] Bala, B., Kamboj, L., & Luthra, P. (2018). Secure file Storage in Cloud Computing Using Hybrid Cryptography Algorithm. International Journal of Advanced Research in Computer Science, 9(2).

[26] I. T. Singh, T. R. Singh and T. Sinam, "Server Load Balancing with Round Robin Technique in SDN," 2022 International Conference on Decision Aid Sciences and Applications (DASA), Chiangrai, Thailand, 2022, pp. 503-505, doi: 10.1109/DASA54658.2022.9765287.

[27] X. Yu, H. Hou and G. Han, "Comparison on Vandermond and Cauchy MDS Array Codes in Distributed Storage Systems," 2020 2nd World Symposium on Artificial Intelligence (WSAI), Guangzhou, China, 2020, pp. 11-17, doi: 10.1109/WSAI49636.2020.9143308.

[28] L. Bannawat, A. Boonpoonga and S. Burintramart, "Detection and Classification of Buried Improvised Explosive Devices using Cauchy Method," 2018 18th International Symposium on Communications and Information Technologies (ISCIT), Bangkok, Thailand, 2018, pp. 514-518, doi: 10.1109/ISCIT.2018.8587955.

[29] Guangyan Zhang, Guiyong Wu, Shupeng Wang, Jiwu Shu, Weimin Zheng, and Keqin Li, "CaCo: An Efficient Cauchy Coding Approach for Cloud Storage Systems," IEEE Transactions on computers, Vol.62, No.11, November 2015.

[30] S. Ren, Q. -M. Cai, X. Cao, B. Luo, Y. Zhu and J. Fan, "Design of High Performance Reed-Solomon Encoder Based on A Novel Half-multiplier," 2022 International Applied Computational Electromagnetics Society Symposium (ACES-China), Xuzhou, China, 2022, pp. 1-2, doi: 10.1109/ACES-China56081.2022.10065001.

[31] V. R. Ch, R. Sankar Miriyala, P. V, V. B. Sri, B. Sri Sailesh A and R. K, "Performance Evaluation of OFDM System: With and Without Reed-Solomon Codes," 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2022, pp. 1827-1831, doi: 10.1109/ICAC3N56670.2022.10074060.

[32] A. Aspreas and K. Yiannopoulos, "Bit Error Probability of an Optically Pre-amplified Pulse Position Modulation Receiver with Reed Solomon Error Correction," 2022 Panhellenic Conference on Electronics & Telecommunications (PACET), Tripolis, Greece, 2022, pp. 1-5, doi: 10.1109/PACET56979.2022.9976360.

[33] Z. Jiang, "Performance Analysis of Utilizing Reed Solomon Code in Redundant Array of Independent Disk," 2022 International Symposium on Advances in Informatics, Electronics and Education (ISAIEE), Frankfurt, Germany, 2022, pp. 69-72, doi: 10.1109/ISAIEE57420.2022.00022.

[34] R. Con, A. Shpilka and I. Tamo, "Reed Solomon Codes Against Adversarial Insertions and Deletions," 2022 IEEE International Symposium on Information Theory (ISIT), Espoo, Finland, 2022, pp. 2940-2945, doi: 10.1109/ISIT50566.2022.9834672.

[35] Ghazal R, Malik AK, Qadeer N, Raza B, Shahid AR, Alquhayz H. Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments. IEEE Access. 2020 Jan 9;8:12253-67.

[36] J. Surbiryala and C. Rong, "Data Recovery and Security in Cloud," 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA), Zakynthos, Greece, 2018, pp. 1-5, doi: 10.1109/IISA.2018.8633640.

[37] A. Mathew and C. Mai, "Study of Various Data Recovery and Data Back Up Techniques in Cloud Computing & Their Comparison," 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2018, pp. 2021-2024, doi: 10.1109/RTEICT42901.2018.9012485