IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

Reversible Data Hiding with Multiple Secret Sharing Using Cryptography Approach

Mr. K. Jeeva[1], G. Dhanavarsha[2], K. Nanthini[3]
Assistant Professor, Department of Internet of Things[1]
Students, Department of Information Technology[2,3]
Dhanalakshmi Srinivasan University, Samayapuram, Thiruchirapalli, Tamilnadu, India

Abstract: *Visual Cryptography (VC) is used to break an image into two random shares which when separately viewed reveals no information about the secret image. The secret image can be obtained by super imposing the two shares. Conventional visual cryptography scheme is used to encrypt a single image into n shares. The image can be decoded by using only shares. Many visual cryptographic methods use binary images only for this process. A sufficient condition to be satisfied by the encryption of MSS (Multiple Secret Sharing) schemes realizing an access structure for multiple secrets of the most general form is introduced, and two constructions of MSS schemes with encryption satisfying this condition are provided. Each of the two constructions has its advantage against the other; one is more general and can generate MSS schemes with strictly better contrast and pixel expansion than the other, while the other has a straightforward implementation. The main objective of this project is to establish a secured communication between the sender and the receiver by using emails and other communicating modes. In this work, an ECC based multi secret sharing is proposed to send secret information from the source to the destination in a secured way. The secret text was hidden within the image. The image is hidden inside an image using Modified LSB methodology. Then image is splited into shares and encrypted using ECC method. The proposed method is n out of n multi secret sharing scheme. Transmission of multiple secret images simultaneously is achieved through this proposed work. The secret image can be revealed only when all the n shares are received by the receiver and decrypted. At the receiver end, the hidden data is extracted from the recovered image. Experimental results show that the dimensions of the original image and the recovered image are same.*

Keywords: Visual Cryptography, Multi-Secret Sharing (MSS), Elliptic Curve Cryptography (ECC), Image Encryption, Secure Communication, Data Hiding, Cryptographic Security

I. INTRODUCTION

Visual Cryptography (VC) is a powerful technique used to secure images by breaking them into multiple random shares, ensuring that no individual share reveals any information about the secret image. The secret image can only be reconstructed by superimposing the shares. Traditional visual cryptography methods primarily focus on encrypting a single image into multiple shares, typically supporting only binary images. However, such limitations make conventional approaches unsuitable for many real-world applications. This project introduces a Multiple Secret Sharing (MSS) scheme, transforming the encryption process from a single-secret structure to one that supports multiple secrets. The proposed method integrates Elliptic Curve Cryptography (ECC)-based multi-secret sharing, where secret information is embedded within an image. A Modified Least Significant Bit (LSB) methodology is used to hide the image inside another image before it is split into multiple shares and encrypted using ECC. This approach follows an n-out-of-n secret sharing scheme, where all shares are required to reconstruct the original image. Only when all shares are received and decrypted can the hidden data be extracted from the recovered image.

DOI: 10.48175/IJARSCT-26413

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

II. RESEARCH PROBLEM

The core research problem addressed in this project lies in overcoming the limitations of traditional visual cryptography, which typically supports only binary images and single-secret scenarios, making it impractical for complex, real-world applications involving high-resolution images and multiple pieces of sensitive information. There is a critical need for a more advanced and secure visual cryptography system that enables the sharing and protection of multiple secrets simultaneously while maintaining image quality and reducing computational overhead. This project tackles these issues by proposing a novel Multiple Secret Sharing (MSS) scheme that integrates Elliptic Curve Cryptography (ECC) for robust encryption and a Modified Least Significant Bit (LSB) approach for efficient steganography. The challenge lies in designing an encryption framework that ensures high security, supports multi-secret handling, maintains visual integrity, and enables full recovery of hidden data only when all shares are present—thus strengthening secure communication over unreliable or unsecured channels such as email.

III. LITERATURE REVIEW

Sekar, Jeyasri
Year: 2023
This proposed system's primary goal is to enhance the performance, scalability, and reliability of AI workflows by leveraging the strengths of multiple cloud service providers. The approach involves designing a comprehensive framework that integrates various multi-cloud strategies tailored for distributed AI workflows. The framework is implemented and tested using real world AI applications across different cloud environments. Performance metrics such as latency, throughput, and cost-efficiency are used to evaluate the effectiveness of the proposed strategies. The study reveals that multi-cloud strategies significantly improve the overall performance and resilience of distributed AI workflows. Key findings indicate a reduction in latency by up to 30%, an increase in throughput by 25%, and cost savings of approximately 20% compared to single-cloud deployments. Additionally, the flexibility to dynamically switch between cloud providers based on workload demands enhances reliability and fault tolerance. Future work will focus on refining the framework and exploring advanced orchestration techniques to further enhance multi-cloud AI workflows.

Krishnasamy, KamalamGobichettipalayam
Year: 2023
Scheduling tasks to distributed heterogeneous clouds is termed NP-complete which leads to the ultimate establishment of heuristic problem solving technique. Group 1 comprises ($[n/2]$) tasks ordered in descending value of threshold. Group 2 comprises remaining tasks ($[n/2]-1$) ordered in ascending value of threshold. Secondly, tasks form group 1 are scheduled first based on minimum completion time, and then tasks in group 2 are scheduled. The proposed approaches PTL, PTMax-Min, and PTMin-Max explicitly shows the better results in terms of reduced makespan, completion time, response time and more resource utilization compared to MCT, MET, and Min-min.

Thillaiarasu, N., S. ChenthurPandian, and NaveenbalajiGowthaman Year: 2022
Safety is the main concern and also it acts as a major hurdle in maintaining cloud-based services. Apart from these safety issues, the cloud holds a collection of different features and frameworks. Such types of cloud frameworks are set off, and their safety, confidentiality, and probabilities are discussed in this chapter. The proposed technique offers a reduction of 0.3% and 5.62% system time for creating a directory for 10k and 20k files, respectively, when compared to the conventional B-Tree technique.

IV. SYSTEM REQUIREMENTS

FUNCTIONAL REQUIREMENTS

This section outlines the functional requirements essential for implementing and evaluating the Multi-Secret Sharing (MSS) system for secure information distribution among authorized participants. The system integrates multiple layers of secret data (such as biometric keys, encrypted credentials. It must provide robust protection against unauthorized

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

access, support dynamic participant management, and ensure data integrity, confidentiality, and enhanced resilience against data breaches or compromise.

SOFTWARE REQUIREMENTS

- Operating system : Windows OS
- Front End : Html, CSS
- Back End : Python
- Database : My sql
- IDLE : Python 2.7 IDLE

PYTHON

Python is an interpreted high-level programming language for general-purpose programming. Created by Guido van Rossum and first released in 1991, Python has a design philosophy that emphasizes code readability, notably using significant whitespace. In July 2018, Van Rossum stepped down as the leader in the language community. Python features a dynamic type system and automatic memory management. Python's initial development was spearheaded by Guido van Rossum in the late 1980s. Today, it is developed by the Python Software Foundation.

MY SQL

MySQL is the world's most used open source relational database management system (RDBMS) as of 2008 that run as a server providing multi-user access to a number of databases. Applications which use MySQL databases include: TYPO3, Joomla, Word Press, phpBB, MyBB, Drupal and other software built on the LAMP software stack. MySQL is also used in many high-profile, large-scale World Wide Web products, including Wikipedia, Google(though not for searches), ImagebookTwitter, Flickr, Nokia.com, and YouTube.

Interimages

MySQL is primarily an RDBMS and ships with no GUI tools to administer MySQL databases or manage data contained within the databases. Users may use the included command line tools, or use MySQL "front-ends", desktop software and web applications that create and manage MySQL databases, build database structures, back up data, inspect status, and work with data records. The official set of MySQL front-end tools, MySQL Workbench is actively developed by Oracle, and is freely available for use.

Graphical

The official MySQL Workbench is a free integrated environment developed by MySQL AB, that enables users to graphically administer MySQL databases and visually design database structures. MySQL Workbench replaces the previous package of software, MySQL GUI Tools. MySQL Workbench is available in two editions, the regular free and open source Community Edition which may be downloaded from the MySQL website, and the proprietary Standard Edition which extends and improves the feature set of the Community Edition.

Command line

MySQL ships with some command line tools. Third-parties have also developed tools to manage a MySQL server, some listed below.

MySQL works on many different system platforms, including AIX, BSDi, FreeBSD, HP-UX, eComStation, i5/OS, IRIX, Linux, Mac OS X, Microsoft Windows, NetBSD, Novell NetWare, OpenBSD, OpenSolaris, OS/2 Warp, QNX, Solaris, Symbian, SunOS, SCO OpenServer, SCO UnixWare, Sanos and Tru64. A port of MySQL to OpenVMS also exists. MySQL is written in C and C++. Its SQL parser is written in yacc, and a home-brewed lexical analyzer.

- A broad subset of ANSI SQL 99, as well as extensions
- Cross-platform support

DOI: 10.48175/IJARSCT-26413

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

- Stored procedures
- Triggers
- Cursors
- Updatable Views
- Information schema
- Strict mode (ensures MySQL does not truncate or otherwise modify data to conform to an underlying data type, when an incompatible value is inserted into that type)
- X/Open XAdistributed transaction processing (DTP) support; two phase commit as part of this, using Oracle's InnoDB engine
- Independent storage engines (MyISAM for read speed, InnoDB for transactions and referential integrity, MySQL Archive for storing historical data in little space)
- Transactions with the InnoDB, and Cluster storage engines; savepoints with InnoDB
- SSL support
- Query caching
- Sub-SELECTs (i.e. nested SELECTs)
- Full-text indexing and searching using MyISAM engine
- Embedded database library
- Unicode support (however prior to 5.5.3 UTF-8 and UCS-2 encoded strings are limited to the BMP, in 5.5.3 and later use utf8mb4 for full unicode support)
- ACID compliance when using transaction capable storage engines (InnoDB and Cluster)
- Partititoned tables with pruning of partitions in optimiser
- Shared-nothing clustering through MySQL Cluster
- Hot backup (via mysqlhotcopy) under certain conditions

HARDWARE REQUIREMENTS

- Processor : Intel core processor 2.6.0 GHZ
- RAM : 4 GB
- Hard disk : 320 GB
- Compact Disk : 650 Mb
- Keyboard : Standard keyboard
- Monitor : 15 inch color monitor

V. SYSTEM DESIGN AND IMPLEMENTATION

Proposed Solution

The proposed system enhances traditional visual cryptography by introducing a Multiple Secret Sharing (MSS) scheme that ensures secure transmission of confidential data through encrypted image shares. This approach integrates Elliptic Curve Cryptography (ECC) for encryption and a Modified Least Significant Bit (LSB) methodology for data hiding, providing a robust and efficient solution for secure communication. Unlike conventional methods that primarily support binary images, this system enables the encryption and transmission of multiple secret images while maintaining image quality and security. In the encryption phase, the secret information is first embedded within an image using the Modified LSB technique. This embedded image is then divided into multiple random shares, ensuring that no single share contains meaningful information. Each share is further encrypted using ECC to enhance security. This advanced approach enhances security, data integrity, and confidentiality, making it an effective solution for secure data transmission in various applications.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

Advantages

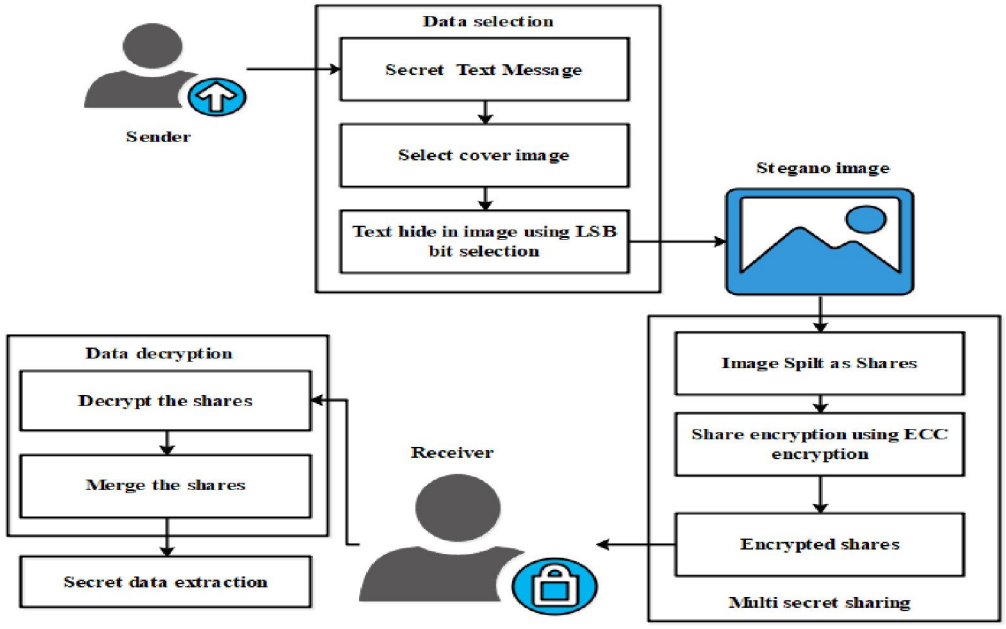
- The secret image and the recovered image will be of the same size.
- Multi secret sharing is used to send multiple shares at the same time.
- Enhance security with ECC algorithm.
- To retain the quality of the recovered image.

SYSTEM ARCHITECTURE

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADLs).

Various organizations define systems architecture in different ways, including:

- An allocated arrangement of physical elements which provides the design solution for a consumer product or life-cycle process intended to satisfy the requirements of the functional architecture and the requirements baseline.
- Architecture comprises the most important, pervasive, top-level, strategic inventions, decisions, and their associated rationales about the overall structure (i.e., essential elements and their relationships) and associated characteristics and behavior.
- If documented, it may include information such as a detailed inventory of current hardware, software and networking capabilities; a description of long-range plans and priorities for future purchases, and a plan for upgrading and/or replacing dated equipment and software
- The composite of the design architectures for products and their life-cycle processes.



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

MODULES DESCRIPTION

MODULES LIST

- ENROLMENT AND FILE SHARING
- IMAGE UPLOAD AND HIDING
- FILE ENCRYPTION
- MULTI SHARE SENDING
- SHARE DECRYPTION AND DATA EXTRACTION

Enrolment and File Sharing

Enrolment is the process of registering in application to get access permission. Then sender could create text message for sharing to the receiver. The secret text message hiding is a process of embedding the secret text imperceptibly into the cover media by minimally modifying the elements of the cover media. In this module sender will generate the content for transmit to the receiver. User input text can be converted into QR code.

Image Upload and Hiding

This process is to select cover media for information hiding. Here images are used as a cover media for the secret message. Cover image is also select by the sender when create the secret message. Original message is hidden into the cover media (image) to improve the security of data sharing. This is done by using modified LSB method. The cover image is called as a steganography image.

Elliptic Curve Cryptography (ECC) is a powerful encryption technique that provides **strong security with minimal computational overhead**, making it ideal for encrypting sensitive files. The encryption process begins by converting the file into a set of numerical values, which are then mapped onto points on an elliptic curve. Using a **public-private key pair**, the data points are encrypted, ensuring that only an authorized receiver with the correct private key can decrypt the file.

Multi Share Sending

All the individual encrypted shares will be stored in a folder. By using this module, all the encrypted shares will be sent to the receiver in a single transmission. This single transmission enables receiver to receive all the shares at a time. This will help to avoid the information or share missing and also it saves transmission and receiving time for both sender and receiver.

Share Decryption and Data Extraction

All the encrypted shares will be received by the receiver in a single transmission. Each received share will be decrypted individually using inverse XOR method. The key that is received through mail is used in this decryption process. Private key is used for both encryption and decryption process. The output of this module will be an individual share in the decrypted form.

VI. SYSTEM TESTING AND VALIDATION

EVALUATION METRICS

To assess the effectiveness and performance of the proposed Multiple Secret Sharing (MSS) visual cryptography system, several evaluation metrics are utilized. Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) are used to measure the quality of the reconstructed image in comparison to the original image, ensuring minimal distortion after embedding and recovery. A higher PSNR and SSIM value indicates better image quality preservation. Bit Error Rate (BER) is evaluated to determine the accuracy of the recovered secret data, where a lower BER reflects fewer errors in data extraction. Encryption Time and Decryption Time are measured to analyze the computational efficiency of the system, ensuring that the use of ECC and LSB techniques does not introduce significant delays. Security Analysis is conducted to validate the system's resistance to common attacks such as brute-force,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

differential, and statistical analysis. Additionally, Share Randomness and Independence are evaluated to ensure that individual shares do not leak any information and are statistically independent. These metrics collectively help demonstrate that the system is not only secure and accurate but also efficient and practical for real-world applications.

Correctness:

The correctness of the proposed system is primarily concerned with ensuring that the secret image is correctly embedded, transmitted, and reconstructed without any loss of data or quality. The system must reliably embed the secret data into the cover image, divide it into shares, and ensure that, upon successful decryption and reconstruction, the original image and embedded secrets can be fully recovered. To validate correctness, the system performs the following steps in a sequential manner:

1. **Embedding Stage:** The secret image is embedded into the cover image using the Modified LSB technique. The system verifies that the secret data is correctly embedded without perceptible distortion.
2. **Share Generation Stage:** The embedded image is divided into multiple random shares. The system checks that no single share reveals any meaningful data.
3. **Encryption Stage:** Each share is encrypted using ECC, and the system ensures that the encryption process completes successfully and securely.
4. **Transmission and Decryption Stage:** Upon receiving all encrypted shares, the system decrypts each share using ECC and checks that the decryption is performed correctly without errors.
5. **Reconstruction Stage:** The system verifies that the reconstructed image is identical to the original image, confirming that the embedded secret data can be accurately extracted.

Error Rate:

The error rate in the proposed system is an essential metric to evaluate the reliability and accuracy of the image encryption, transmission, and reconstruction processes. It quantifies the discrepancy between the original secret image and the reconstructed image after the system has performed embedding, encryption, and decryption. The error rate is typically measured using Bit Error Rate (BER), which calculates the percentage of pixels or bits that are incorrect in the reconstructed image compared to the original image. A lower error rate indicates higher accuracy and successful data recovery, while a higher error rate signifies potential problems in the encryption, transmission, or reconstruction process. The system must ensure that the BER is as low as possible to guarantee the integrity of the hidden data. This includes ensuring that the Modified LSB technique and ECC encryption do not introduce significant data loss during embedding and decryption. To achieve this, the error rate function checks for discrepancies between the original image and the reconstructed image at every stage, from embedding to extraction.

Latency:

Latency refers to the time delay between the initiation of a request (such as sending an encrypted image share) and the completion of the corresponding operation (such as the reception and reconstruction of the image). In the context of this project, latency is a critical performance metric that helps evaluate the efficiency of the proposed encryption and decryption system. This metric measures the time taken for the encrypted shares to be transmitted, received, decrypted, and then reconstructed into the original image. Latency can be influenced by multiple factors, including the complexity of the encryption/decryption algorithms, the size of the images being transmitted, network conditions, and the number of shares involved in the encryption process.

A key challenge in this project is balancing the need for high security (through Elliptic Curve Cryptography (ECC) and Modified Least Significant Bit (LSB)) with the requirement for low latency, especially when dealing with large image files and multi-cloud or multi-channel transmissions. The proposed system must optimize the encoding and transmission stages to minimize delays while maintaining security standards.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

MODEL EVALUATION TESTING

Testing is a set activity that can be planned and conducted systematically. Testing begins at the module level and work towards the integration of entire computers-based system. Nothing is complete without testing, as it is vital success of the system.

Testing Objectives:

There are several rules that can serve as testing objectives, they are

- Testing is a process of executing a program with the intent of finding an error
- A good test case is one that has high probability of finding an undiscovered error.
- A successful test is one that uncovers an undiscovered error.

If testing is conducted successfully according to the objectives as stated above, it would uncover errors in the software. Also testing demonstrates that software functions appear to the working according to the specification, that performance requirements appear to have been met.

There are three ways to test a program

- For Correctness
- For Implementation efficiency
- For Computational Complexity.

Tests used for implementation efficiency attempt to find ways to make a correct program faster or use less storage. It is a code-refining process, which reexamines the implementation phase of algorithm development. Tests for computational complexity amount to an experimental analysis of the complexity of an algorithm or an experimental comparison of two or more algorithms, which solve the same problem.

The data is entered in all forms separately and whenever an error occurred, it is corrected immediately. A quality team deputed by the management verified all the necessary documents and tested the Software while entering the data at all levels.

TYPES OF TESTING

The development process involves various types of testing. Each test type addresses a specific testing requirement. The most common types of testing involved in the development process are:

- Unit Test
- Functional Test
- Integration Test
- White box Test
- Black box Test
- System Test
- Validation Test
- Acceptance Test

Unit Testing:

The first test in the development process is the unit test. The source code is normally divided into modules, which in turn are divided into smaller units called units. These units have specific behavior. The test done on these units of code is called unit test. Unit test depends upon the language on which the project is developed. Unit tests ensure that each unique path of the project performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Functional Testing:

Functional test can be defined as testing two or more modules together with the intent of finding defects, demonstrating that defects are not present, verifying that the module performs its intended functions as stated in the specification and establishing confidence that a program does what it is supposed to do.

Integration Testing:

DOI: 10.48175/IJARSCT-26413

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

In integration testing modules are combined and tested as a group. Modules are typically code modules, individual applications, source and destination applications on a network, etc. Integration Testing follows unit testing and precedes system testing. Testing after the product is code complete. Betas are often widely distributed or even distributed to the public at large in hopes that they will buy the final product when it is released.

White Box Testing:

Testing based on an analysis of internal workings and structure of a piece of software. This testing can be done sing the percentage value of load and energy. The tester should know what exactly is done in the internal program.

REFERENCES

[1]Sekar, Jeyasri. "Multi-Cloud Strategies For Distributed Ai Workflows And Application." Journal of Emerging Technologies and Innovative Research 10 (2023): P600-P610.

[2] Krishnasamy, KamalamGobichettipalayam, et al. "A pair-task heuristic for scheduling tasks in heterogeneous multi-cloud environment." Wireless Pers

[3] Thillaiarasu, N., S. ChenthurPandian, and NaveenbalajiGowthaman. "Novel heuristic scheme to enforce safety and confidentiality using feature-based encryption in multi-cloud environment (MCE)." Information and Knowledge in Internet of Things (2022): 441-456.

[4] Achar, Sandesh. "Cloud computing security for multi-cloud service providers: Controls and techniques in our modern threat landscape." International Journal of Computer and Systems Engineering 16.9 (2022): 379-384.

[5] Zhu, Qing-Hua, et al. "Task scheduling for multi-cloud computing subject to security and reliability constraints." IEEE/CAA Journal of AutomaticaSinica 8.4 (2021): 848-865.

[6] Desai, Bhavin, and KapilPatil. "Demystifying the complexity of multi-cloud networking." Asian American Research Letters Journal 1.4 (2024).

[7]Nassif, Ali Bou, et al. "Machine learning for cloud security: a systematic review." IEEE Access 9 (2021): 20717-20735.

[8] Parast, FatemehKhoda, et al. "Cloud computing security: A survey of service-based models." Computers & Security 114 (2022): 102580.

[9] Ali, Belal, Mark A. Gregory, and Shuo Li. "Multi-access edge computing architecture, data security and privacy: A review." IEEE Access 9 (2021): 18706-18721.

[10] Alghofaili, Yara, et al. "Secure cloud infrastructure: A survey on issues, current solutions, and open challenges." Applied Sciences 11.19 (2021): 9005