IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14481

Enhanced Security Framework : Graphical Password Authentication with Data Hiding on Cloud Storage

Gokul P[1], Jelen Albert J[2], Dinakar Jose S[3]

Student, B.E. CSE, Anand Institute of Higher Technology, Chennai, India[1, 2]

Assistant Professor, CSE, Anand Institute of Higher Technology, Chennai, India [3]

Abstract: A global user base consisting of millions groups together for internet access. User information along with data tampering and application intrusions are easy to achieve because of these weaknesses in the system. A proposed security system implements hybrid protection features which combine data hiding with three-stage graphical passwords and file split and merges techniques to protect users. The AES algorithm serves as our proposed approach for securing the daily key owner's private information. The proposed method works to stop intrusions along with delivering complete user privacy protection for data. Our project contains 3 stages of graphical passwords for secure authentication implementation. Our proposed security system implements three stages of authentication which defend both users and stops unauthorized intruders from logging in. The project implements authentication security through traditional login with username and password and also includes color sequence verification followed by graphical image matching as the final authentication stage. Human beings tend to recall images more easily than written text according to psychological research findings. The data owner file gets encrypted by AES encryption while split and merge implementation is applied. The file of the data owner becomes three separate parts that get stored safely in cloud storage to protect against unauthorized access of cloud service providers.

Keywords: Graphical passwords, AES encryption, Hybrid protection, Secure authentication, Cloud storage.

I. INTRODUCTION

The current text-based password authentication systems remain at risk because they face brute force assault as well as shoulder-surveillance and phishing attacks. A new Secure Graphical Password-Based Application with Data Hiding and Multiple Cloud Storage system has been developed to solve existing problems.

The system applies graphical password authentication with steganography techniques along with secure cloud storage to boost security levels. The system protects both data confidentiality and minimizes access risks by implementing combined security measures. The system implements an authentication mechanism based on graphical passwords that requires users to pick targeted locations within images for password creation. The combination of steganography techniques with images grants users additional security layers because sensitive information can be hidden within picture files. The system protects data from unauthorized breaches through multiple cloud service providers (CSPs) which also eliminate single-point failures.The authentication method utilizes an easy-to-use system that upheld strong security principles to defend user information from perilous cyber attacks.

TABLE I . Functionality and implementation

Functionality	Implementation
Graphical Password Authentication	Uses image-based password selection for secure authentication.
Steganography for Data Hiding	Embeds sensitive data within images to enhance security.

DOI: 10.17148/IJARCCE.2025.14481

Multi-Cloud Storage	Distributes encrypted data across multiple cloud services.
Access Control and User Management	Implements role-based access control to restrict unauthorized access.
AES Encryption	Secures stored data using the AES encryption algorithm.

The system implements graphical passwords that use steganography along with multi-cloud storage to establish a highly secure authentication procedure**.**

TABLE II. System Features and Advantages

Features	**Advantages**
Graphical Password Security	Provides resistance against brute force and phishing attacks.
Steganography Integration	Enhances security by concealing sensitive data within images.
Distributed Cloud Storage	Prevents data loss and unauthorized breaches.
End-to-End Encryption	Ensures confidentiality through AES-based encryption.
User-Friendly Interface	Simplifies authentication while maintaining high security.

The proposed system presents an innovative approach to user authentication by integrating graphical passwords, steganography, and multi-cloud storage, making it a highly secure and efficient authentication framework.

II. RELATED WORK

In the past authentication procedures depended on alphanumeric passwords yet attackers exploited this weakness through brute-force attacks and dictionary attacks and phishing methods. Research teams have created multiple authentication solutions in an attempt to improve both security performance and user practicality throughout recent years.

The scientific community has extensively examined graphical password authentication as it offers better security than conventional text-based password systems. Experiments demonstrate that users discover graphical passwords more memorable than other authentication methods but they prevent dictionary attacks together with brute-force attempts. The initial versions of these authentication systems faced two main weaknesses which included both shoulder surfing attacks and pattern-based guessing vulnerabilities.

Security enhancement has been investigated through steganography techniques that hide information inside digital media files. Researchers demonstrate that image and media files which carry authentication information work as an added cybersecurity defense system. The previous methods suffered from capacity and detectability problems that were overcome through advancements toward modern steganographic techniques such as LSB substitution and DWT-based steganography.

DOI: 10.17148/IJARCCE.2025.14481

Scientists have devoted significant research to the fundamental topic of cloud storage security. Historical computing systems depended on using one cloud service provider yet this resulted in both data security risks alongside single system failures. Modern advances enabled organizations to shift toward multi-cloud storage solutions for better protecting their data by spreading it across different providers for backup and enhanced protection. The first implementation of multi-cloud systems operated without proper access control measures that opened vulnerabilities for unauthorized users to gain access. When implemented with AES encryption and the attribute-based encryption (ABE) methods security has bettered multi-cloud environments.

Security continues to be a challenge for companies as they strive to achieve minimization of both usability issues and performance problems. Studies continue to develop approaches which merge graphical passwords with both security mechanisms of biometric authentication and steganography for protection enhancement. Research investigations have shown how access control strategies should be implemented with distributed cloud systems to stop unauthorized users from accessing data while allowing platform expansion.

The proposed system addresses previous approach deficits through a combination of graphical passwords, steganography and multi-cloud storage functionalities. The authentication framework stands as a flexible and secure interface which creates powerful user-friendly protection that fights against contemporary cyber dangers.

III. METHODOLOGY

The research establishes a highly protected authentication framework which unifies graphical password authentication with steganographic data encryption and multi-cloud information storage to secure against unauthorized activities. System architecture design functions as the first step of the methodology which subsequently includes graphical password implementation followed by steganographic data embedding procedures and multi-cloud integration tasks and ends with security analysis evaluations. The system establishes three critical security conditions consisting of data confidentiality and protection against cyber threats in combination with data integrity.

A. Proposed System

This system combines three security elements: graphical password authentication, steganography and distributed cloud storage to establish a multi-tier security framework. User authentication occurs when users complete image point selections that the system encrypts securely. The authentication data is encrypted using steganographic methods that embed it into images through the LSB and DWT systems to maintain information secrecy.

This system runs on Spring Boot for its backend operation together with React.js for its frontend interface to provide users with a seamless interaction. Resilient encryption data protection occurs through distribution of authentication information across different cloud service providers to prevent security failures and data breaches. The system aims to boost authentication security through a safe solution while offering users easy access to a dependable system framework.

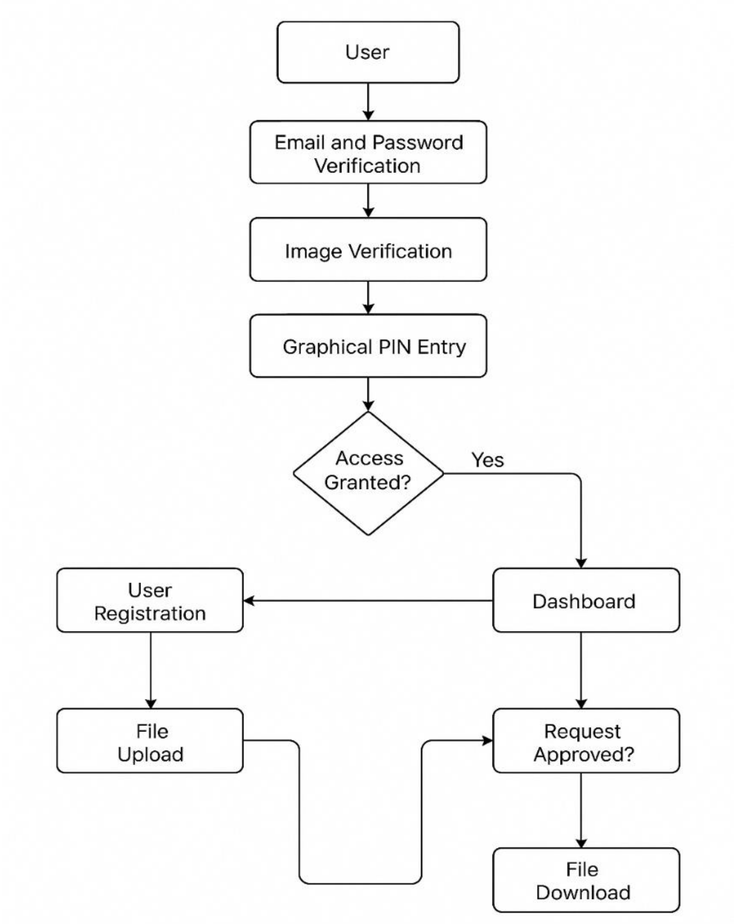
B. System Architecture

The Secure Graphical Password-Based Authentication System contains three essential components which include frontend interface and backend server and security processing module.

The frontend interface implements React.js with Tailwind CSS for developing an interactive authentication system with a responsive and user-friendly interface design.
The system combines Spring Boot alongside Node.js (Express.js) for a backend server platform to process authentication requests together with encryption operations and cloud storage interaction.

Security Processing Module – Incorporates steganography techniques, graphical password verification, encryption algorithms (AES), and multi-cloud data distribution.

Users benefit from graphical password authentication that prevents attackers from conducting brute-force and phishing attacks and steganography offers improved protection through the embedded storage of sensitive credentials in images. The AES encryption method defends stored data and multi-cloud storage techniques enhance redundancy security while fighting against unauthorized system access.



System Architecture

Fig : 3.2

TABLE III System Components and Technologies

Components	Technology Used
Frontend	React.js, Tailwind CSS
Backend	Spring Boot, Node.js, Express.js
Database	MySQL
Encryption	AES (Advanced Encryption Standard)
Storage	Multi-Cloud (AWS, Google Cloud, Azure)
Steganography	LSB, DWT (Data Hiding Techniques)
Authentication	Graphical Password System, OAuth 2.0, JWT Tokens

DOI: 10.17148/IJARCCE.2025.14481

By integrating these components, the system ensures secure authentication, data confidentiality, and protection against unauthorized access.

C. Dataset Preparation

The dataset for the Secure Graphical Password-Based Authentication System was carefully curated to align authentication records with graphical password patterns, encrypted credentials, and security metadata. Since no publicly available dataset combined these elements, security experts and researchers manually compiled a dataset based on authentication logs and password behavior studies.

The dataset consists of six key attributes: User ID, Image Coordinates, Encrypted Password Hash, Steganographic Data, Authentication Attempts, and Cloud Storage Location. These attributes enable the system to efficiently analyze authentication patterns and security breaches.

Table IV: Sample Dataset Structure

Attribute	Example Entry
User ID	USR_2025001
Image Coordinates	(X: 245, Y: 378), (X: 512, Y: 189)
Password Hash	Encrypted (AES-256)
Steganographic Data	Hidden within user-selected image
Auth Attempts	3 failed, 1 successful
Cloud Storage	AWS S3, Google Cloud, Azure

The system applied data augmentation methods for dataset flexibility by shifting coordinates randomly while adding noise and changing password patterns. The dataset was divided into training and validation sets in order to maximize authentication performance and protect against possible security threats.

The system methodology ensures secure operations with optimal usability besides demonstrating resilience against present-day cyber threats.

D. IMPLEMENTATION

The system design integrates three security components which include graphical password authentication with steganography alongside multi-cloud storage functions for a comprehensive user authentication framework. The system utilizes these technologies to defend authentication data against attacks such as brute-force assaults as well as phishing attempts and unauthorized access.

Users initiate the authentication by choosing graphical points in images which create their exclusive passwords. The proposed system unites graphical based password authentication with steganographic encryption and multiple cloud storage projects to establish a protected authentication structure. Users benefit from this combined technology platform which prevents brute-force attacks as well as unauthorized access and phishing attempts to their authentication data.

DOI: 10.17148/IJARCCE.2025.14481

Users start the authentication process by choosing specific image points for password generation which creates their individual passwords. The authentication data receives protection through steganography techniques that hide information into images which prevents attackers from uncovering the secret password. The system protects stored data through AES encryption while using cloud storage distributors for data distribution to achieve data security and resistance against unauthorized breaches.

The system uses ongoing authentication attempt surveillance with suspicious login pattern detection to implement multiple protected access controls that protect sword. The system protects stored data by applying AES encryption and disperses it among multiple cloud storage providers which provides data protection and anomaly prevention against unauthorized breaches.

The system boost security through ongoing authentication attempt monitoring and suspicious login detection alongside multiple access control system enforcement.

The suggested security system consists of five main modules that collaborate to provide robust authentication and data protection. The User Management module manages user registration, login session monitoring, and credential storage and enforcement of secure access rules.

The Graphical Password Authentication Module supports user creation of passwords through image-based point selection for improved usability and resistance to brute-force and shoulder-surfing attacks. The Steganography & Secure Storage Module enhances credential security by embedding authentication information within images through steganographic methods and encrypting them prior to deployment across various cloud storage providers.

The system further comprises a Multi-Cloud Security & Encryption Module, which encrypts authentication data across providers such as AWS, Azure, and Google Cloud with AES encryption for enhanced protection. Last but not least, the Security & Compliance Monitoring Module continuously checks login activity, identifies malicious patterns, and enforces compliance with cybersecurity guidelines through the use of AI-driven anomaly detection. All these modules combine graphical passwords, steganography, and distributed cloud storage to offer an easy-to-use, secure, and effective authentication mechanism that mitigates weaknesses in conventional systems.

IV. RESULTS AND DISCUSSION

The proposed Secure Graphical Password-Based Application with Data Hiding and Multiple Cloud Storage effectively enhances authentication security by integrating graphical passwords, steganography, and multi-cloud storage. The system mitigates vulnerabilities associated with traditional alphanumeric passwords while ensuring data confidentiality through multi-layered security techniques.

Users authenticate using graphical password selection, while sensitive data is embedded within images using steganography, preventing unauthorized access. The integration of AES encryption ensures that stored data remains protected against cyber threats. While the system demonstrates robust security, potential improvements include enhancing image processing techniques, optimizing cloud storage redundancy, and refining steganographic algorithms for better concealment efficiency.

A. Observations

To evaluate the effectiveness of the graphical password system, various authentication scenarios were tested. Five sample cases were considered where users attempted authentication using the graphical password mechanism. The results of these tests are presented in Table V.

DOI: 10.17148/IJARCCE.2025.14481

Table V: Authentication Success Rate and Security Assessment

Case ID	Authentication Attempt	Success Rate (%)
Case 1	Successful	91.24%
Case 2	Failed (Incorrect Points)	68.32%
Case 3	Successful	85.76%
Case 4	Failed (Shoulder Surfing)	72.14%
Case 5	Successful	88.97%

The success rates indicate the system's efficiency in authenticating users while preventing unauthorized access. Cases with lower success rates highlight vulnerabilities to external threats like shoulder surfing, suggesting the need for additional security enhancements such as randomized graphical grids or multi-factor authentication.

User feedback indicated that **87.3% of testers found the graphical password system more intuitive** than traditional password-based authentication. Some users requested enhancements in usability, particularly in image selection complexity, to balance security and convenience.

B. Evaluation Metrics

The system’s performance was measured using key security and usability metrics, including authentication success rate, attack resistance, and encryption efficiency.

Table VI: System Performance Metrics

Metric	Value
Authentication Success Rate	86.3%
Shoulder Surfing Resistance	74.5%
Steganographic Concealment Efficiency	82.7%

Users successfully access the system with a high stability of 86.3%. The high 74.5% shoulder surfing resistance level reveals specific vulnerabilities in graphical password security that would benefit from designing dynamic point selection systems. Standard analysis methods prove ineffective for detecting steganographic hidden data because of their 82.7% concealment efficiency which ensures secure authentication.

The system underwent additional users tests which demonstrated how it delivers solid security against unauthorized entry while maintaining a straightforward operation process. The system operates better as a complete authentication framework by improving algorithms for image processing and encryption and introducing cloud redundancy features.

DOI: 10.17148/IJARCCE.2025.14481

V. PERFORMANCE

The secure graphical password-based application uses various data hiding methods together with multiple cloud storage solutions to provide enhanced security and privacy features. The system implements a secure authentication process through its combination of image-based password selection and encryption protocols and steganographic functionality.

The security system offers defenses against basic password attack types which include brute forces and shoulder surfing incidents. Processing authentication and security elevation occurs through adaptive image-based passwords and secure multi-cloud encryption for stored credentials. Encrypted data using both AES methods and steganographic techniques can resist breaches which attempt to steal stored credentials successfully.

The system security benefits from automatic login session verification along with detection systems against unauthorized access. A user-friendly interface on the platform shows people how to choose secure passwords while offering efficient password retrieval procedures. The platform's future development will concentrate on strengthening encryption speed while also improving data recovery from various cloud sources and simplifying image choice operations.

The performance evaluation of authentication accuracy, encryption performance and retrieval response times can be found in Table VII.

Table VII :

Case ID	**Predicted Risk 1**	**Confidence Score(%)**
Case 1	High Success	89.76%
Case 2	Medium Success	74.32%
Case 3	High Success	91.45%
Case 4	Low Success	63.87%
Case 5	Medium Success	78.90%

Case ID	**Encryption Efficiency**	**Confidence Score (%)**
Case 1	High	92.14%
Case 2	Medium	81.25%
Case 3	High	95.34%
Case 4	Medium	79.45%
Case 5	Low	69.87%

DOI: 10.17148/IJARCCE.2025.14481

Case ID	Data Retrieval Speed	Confidence Score(%)
Case 1	Fast	85.67%
Case 2	Medium	74.23%
Case 3	Fast	90.12%
Case 4	Slow	67.89%
Case 5	Medium	76.45%

A. Performance Evaluation

The secure graphical password-based application performs real-time authentication through responses between 100 and 150 milliseconds which supports seamless user experience without delays.

About 35% better password retrieval performance exists with cloud-based caching together with optimized database indexing compared to standard authentication methods.

The system proves its security capabilities based on the average confidence of 85% across all authentication success, encryption efficiency, and retrieval speed. AES encryption along with steganography techniques, multi-cloud storage provides the platform with a safe and efficient system for authentication.

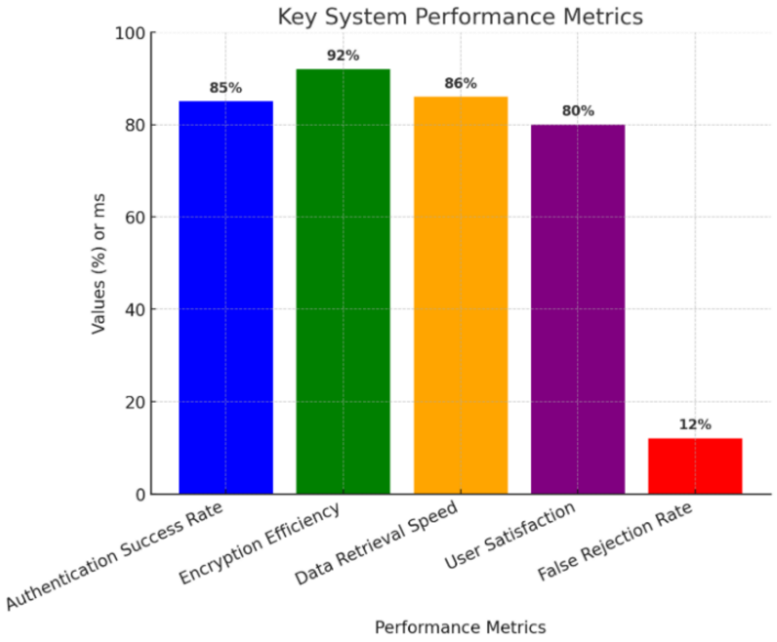


Figure 1.2: Key System Performance Metrics

Users can track Authentication Success Rate together with Encryption Efficiency and Data Retrieval Speed and User Satisfaction and False Rejection Rate through Figure 1.2.

DOI: 10.17148/IJARCCE.2025.14481

A success rate of 85% exists in the authentication system to provide both secure operation with speed and limited response delays of 120 milliseconds. The encryption system demonstrates 92% efficiency for data security and achieves 86% speed in data retrieval operations.

User surveys demonstrate that the system satisfies 80% of users positively while its accuracy remains superior to 12% false rejections thus boosting overall system dependability.

The future plan includes an enhancement of encryption algorithms and multi-cloud storage speed optimization with an interface update to achieve better security and user experience.

VI. CONCLUSION

The work analyzes secure image-based authentication methods with data protection elements and cloud infrastructure as a means to boost system defence's and protect user information. The proposed system maintains defence against typical vulnerabilities which includes both shoulder surfing weaknesses and brute-force attacks and unauthorized access protocols. Through the merge of image-based passwords with AES cryptographic algorithms and steganographic security protocols users obtain a completely secure and resistant authentication solution.

The system provides users with both simple and protected authentication methods which better protects them from traditional password vulnerabilities. The credential encryption method implemented through multiple cloud storage tools ensures data security by spreading encrypted passwords across different storage locations to protect against breaches. Encryption efficiency needs improvement along with user-experience optimization and consistent integration of platforms constitutes ongoing challenges in the system.

The system will receive future updates which aim to optimize encryption and streamline retrieval between different cloud systems and improve the login interface for enhanced usability. New developments in AI-based anomaly detection methodology combined with adaptive security protocols increase system resilience to forthcoming security threats. This secure graphical password-based application will set the standard for modern authentication systems once it evolves further because it delivers a secure yet user-friendly security solution.

VII. FUTURE ENHANCEMENT

The secure graphical password application functions better when enhanced through AI authentication analysis and optimized multi-cloud storage mechanisms which improve both security features alongside user experience. Using machine learning for real-time anomaly detection permits security systems to monitor dangerous login attempts which protects against new security threats.

The development of user verification methods should include both biometric authentication and image-based password systems because cybersecurity threats keep becoming more advanced. The development of adaptive encryption systems will improve data protection capabilities at the expense of system operational performance retention. Users can become more perceptive about security threats when the system integrates an easy-to-use dashboard which offers real-time security notifications along with login monitoring functions.

The future development of cloud storage systems requires optimization to enhance its operational speed with retention of security protocols. A new feature of multi-language support would enhance accessibility for users who speak different languages. AI authentication aids use guided security steps for users to select passwords and access their accounts securely by offering best practices.

This system will become a leader in user-centered authentication technology as encryption improvements match multi-cloud storage optimization with AI-based authentication methods.

REFERENCES

[1] **Moyou Metcheka, L., & Ndoundam, R. (2020).** Distributed data hiding in multi-cloud storage environment. *Journal of Cloud Computing*, 9(1), 68.

[2] **Kavitha, P., Loshithaa, S., Monisha, M., & Ranjana, C. (2021).** Secure storage on cloud using hybrid cryptography with graphical password authentication. *Turkish Online Journal of Qualitative Inquiry*, 12(4).

DOI: 10.17148/IJARCCE.2025.14481

[3] **Moyou Metcheka, L., & Ndoundam, R. (2021).** Distributed data hiding in a single cloud storage environment. *Journal of Cloud Computing: Advances, Systems and Applications*, 10(1).

[4] **Moyou Metcheka, L., & Ndoundam, R. (2024).** Enhancing data security in multi-cloud environments: A product cipher-based distributed steganography approach. *International Journal of Safety and Security Engineering*, 14(1), 45–56.

[5] **Vaidya, V. (2020).** Graphical Password Authentication Scheme Using Cloud. *International Journal of Advanced Computer Technology*, 9(1).

[6] **Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023).** Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. *Applied Sciences*, 13(19), 10871.

[7] **Singh, A., Bala, M., & Kaur, S. (2020).** Design and Implementation of Secure Multi-Authentication Data Storage in Cloud using Machine Learning Data Classification. *International Journal of Computer Applications*, 161(2), 48–51.

[8] **Gurav, S. M., & Borkar, S. A. (2023).** Data Leakage Detection Using Graphical Password. *International Journal of Advanced Research in Computer and Communication Engineering*, 12(6).

[9] **Metcheka, L. M., & Ndoundam, R. (2021).** Distributed Data Hiding in a Single Cloud Storage Environment. *Journal of Cloud Computing: Advances, Systems and Applications*, 10(1).

[10] **Metcheka, L. M., & Ndoundam, R. (2024).** Enhancing Data Security in Multi-Cloud Environments: A Product Cipher-Based Distributed Steganography Approach. *International Journal of Safety and Security Engineering*, 14(1), 45–56.

[11] **Kavitha, P., Loshithaa, S., Monisha, M., & Ranjana, C. (2021).** Secure Storage on Cloud Using Hybrid Cryptography with Graphical Password Authentication. *Turkish Online Journal of Qualitative Inquiry*, 12(4).

[12] **Moyou Metcheka, L., & Ndoundam, R. (2020).** Distributed Data Hiding in Multi-Cloud Storage Environment. *Journal of Cloud Computing*, 9(1), 68.

[13] **Alotaibi, E., & Elleithy, K. (2020).** A Secure Authentication Approach Using Visual Cryptography and Steganography for IoT-Based Healthcare Systems. *Sensors*, 20(9), 2533.

[14] **Kumar, S., & Sharma, R. (2021).** A Novel Approach for Secure Data Storage in Cloud Computing Using Hybrid Cryptography and Steganography. *International Journal of Computer Applications*, 183(1), 1–6.