National College of Ireland

Implementing Robust Data Encryption and Security Measures in Cloud Storage Environments with an Enhanced Cryptographic Layer and Grey Wolf Optimization (ECL-GWO)

MSc Research Project
Cloud Computing

Devaswaroopa Machenahalli Nandish
Student ID: 22169245

School of Computing
National College of Ireland

Supervisor: Dr Ahmed Makki

National College of Ireland
Project Submission Sheet
School of Computing

National College of Ireland

Student Name:	Devaswaroopa Machenahalli Nandish
Student ID:	22169245
Programme:	Cloud Computing
Year:	2023
Module:	MSc Research Project
Supervisor:	Dr Ahmed Makki
Submission Due Date:	14/12/2023
Project Title:	Implementing Robust Data Encryption and Security Measures in Cloud Storage Environments with an Enhanced Cryptographic Layer and Grey Wolf Optimization (ECL-GWO)
Word Count:	7113
Page Count:	25

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Devaswaroopa Machenahalli Nandish
Date:	14th December 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Implementing Robust Data Encryption and Security Measures in Cloud Storage Environments with an Enhanced Cryptographic Layer and Grey Wolf Optimization (ECL-GWO)

Devaswaroopa Machenahalli Nandish
22169245

Abstract

Computing that is done over the internet, or "cloud computing," is a relatively recent innovation. In cloud computing keeping data private, secure, anonymous, and reliable are just some of the cloud's most pressing issues. The most crucial aspect is the security and how the cloud service provider guarantees it. The proposed framework aims to address these challenges by providing a comprehensive data protection solution that incorporates both encryption and optimization techniques. The framework uses the ECL algorithm to optimize the selection of cryptographic keys and the Grey Wolf Optimization (GWO) technique to optimize the placement of data in the cloud. By doing so, the framework is designed to enhance data confidentiality, integrity, and availability in cloud environments while minimizing the risk of security breaches and other types of attacks. Based on the varying opinions of cloud users, this study proposes a Grey Wolf Optimization (GWO) model for addressing privacy issues in the cloud by employing encryption algorithms to enhance the security. The ECL-GWO technique aims to improve the performance and efficiency of data encryption and decryption in cloud environments by optimizing the key generation processes like PBKDF2 and Argon2 key generators. Data integrity ensures by evaluate the performance of ECL and ECL-GWO algorithm with the different workflows. This study examines the potential benefits and drawbacks of using an encryption algorithm in cloud storage to safeguard sensitive data. Proposed approach improve the mitigate of man in the middle attack, so it improves security and authentication. Data security achieved with the proposed ECL GWO algorithm uses encryption to secure data before it is stored on the server and it guarantees that the data can only be accessed by authorized individuals that possess the decryption keys. The GWO algorithm can be used to optimize the security parameters of the encryption algorithm used by the ECL-GWO algorithm. The proposed algorithm was able to enhance the security strength, encryption and decryption time was observed making the encryption and decryption more stable and more over key size is improved resulting in optimized better security.

.

1 Introduction

Cloud computing has become popular, especially for businesses of all sizes. However, Jangjou and Sohrabi (2022)security concerns are a major obstacle to widespread adoption.

Cloud computing's architecture uses new services and technologies that have not been thoroughly tested for security. As a result, there are a number of important challenges and concerns related to cloud computing, including data security, privacy, trust, expectations, regulation, and performance issues.

The security of data in cloud conditions is critical in the present technologically progressed world. Solid data encryption and safety efforts are vital because of the developing dependence on cloud administrations. An enhanced cryptographic layer and grey wolf optimization (ECL-GWO) methodology is introduced in this study to resolve this elementary issue. The chief need of attention is the feebleness of current encryption methods in cloud conditions, requiring novel data security measures Jeniffer and Chandrasekar (2022). Through the consolidation of ECL-GWO, the essential goal of this study is to improve information encryption in cloud conditions. As a means of addressing the shortcomings of the security measures that are currently in place, a new cryptographic layer that is supported by the optimization capabilities of the Grey Wolf Optimization algorithm is proposed by this study. The implementation and evaluation of ECL-GWO are the primary focuses of the research Chourasia and Silakari (2021). The study holds promise for elevating the security paradigm in light of the rapid development of cloud technologies. Hence, the study aims to contribute to the on-going discussion on improving data security in cloud environments as the digital landscape is changing.

1.1 Background

The multiplication of distributed computing addresses a change in outlook in the capacity and handling of information, reshaping the scene of data innovation. The coming of cloud administrations has certainly changed how organizations oversee and get to their information, offering remarkable versatility and adaptability. However, despite the benefits provided by cloud technology, sensitive data security in these environments is still a major concern. Traditional encryption techniques, when considered are found to be stall in defending data. Due to the dynamic nature of cyber threats and the increasing sophistication of malicious actors, these conventional methods have been exposed as vulnerable. A re-assessment of data security methodologies is expected because of the intrinsic shortcoming of customary encryption techniques notwithstanding developing threats such as misuse of the data.

While distributed computing offers parallel convenience, the stake of sensitive information being compromised calls for a novel arrangements. The incorporation of an ECL-GWO as a promising path for strengthening cloud information security emerges within this context Joseph and Mohan (2022). The possibility of an enhanced cryptographic layer keeps an eye on the obstructions of ordinary encryption by introducing a layer of refinement and flexibility. This improvement attempts to strengthen the security position in the cloud conditions by combining advanced cryptographic systems. Such systems go past the conventional procedures, changing in accordance with the creating dangerous scene and giving a more grounded shield against unapproved access and data breaches.

A nature inspired algorithm known as grey wolf optimization (GWO) to which addition of one more layer of development is proposed by the study draws its inspiration from the socially ordered progression and hunting conduct of the grey wolves. GWO soothes out the period of cryptographic keys by mimicking the cooperative and competitive dynamics of wolf packs. GWO enhances the security framework and adds a new dimension

to the process of creating cryptographic keys. ECL-GWO's combination is something beyond the juxtaposition of different parts; it is proposed as the union cooperates to tackle the issues with cloud information security. The algorithm brings adaptability and strength, while the GWO contributes adequacy and upgrade to key age Sajan et al. (2022). Together, these parts structure a careful technique to support data encryption in cloud conditions. This study's motivation lies in its capability to modify distributed computing's information security scene. As an ever increasing number of organizations shift their activities to the cloud, it's a higher priority than any time in recent memory to have adaptable and viable safety efforts. ECL-GWO stays as a showing of the proactive journey for inventive responses for shield sensitive data.

1.2 Motivation of the study

I want to look into this topic for two main reasons. First, more and more people are relying on cloud services to store and get their data. This makes the risks of having weak passwords higher. There's a big problem with identity theft, unauthorized access, and data breaches. This shows we really need to make cloud passwords more secure. Second, even though we've made progress in cloud technology and keeping information safe, we still don't fully know how to use these tools to make passwords stronger in everyday situations.

Securing data in the cloud has become more crucial than ever, given our increasing dependence on digital storage. Confronted with the growing complexity of cyber threats, traditional methods of data protection may prove insufficient. In response to this challenge, our research aims to develop an advanced security approach known as Enhanced Cryptographic Layer (ECL), coupled with Grey Wolf Optimization (GWO). Drawing inspiration from the collaborative nature of grey wolves, we aim to optimize and strengthen data encryption in cloud environments. This research is fueled by the necessity for a more robust and adaptable security solution to effectively safeguard sensitive information, addressing the evolving challenges of data protection in the modern era.

1.3 Problem Statement

Current encryption methods employed in cloud environments may lack the necessary robustness to effectively counteract innovative digital threats. The challenge lies in enhancing security measures to safeguard the confidentiality and integrity of cloud-based information. This study identifies a critical gap in existing encryption techniques and proposes a strategic solution through the integration of ECL-GWO. This sophisticated approach harnesses the optimization capabilities of the Grey Wolf optimizer algorithm combined with an enhanced cryptographic layer, providing a targeted and effective response to fortify data security in the face of creative and evolving cyber threats.

1.4 Objectives

The study's primary objective is to improve security measures and guarantee data confidentiality and integrity in a cloud setting along with the following:

- To enhance data encryption in clouds through the enhancement of the cryptographic layer for grey wolf optimizer and formulate the ECL-GWO based strategy.

- To compare the proposed ECL-GWO approach's performance and security capabilities with traditional algorithms such as Argon2 and Password-Based Key Derivation Function 2 (PKDBK2).
- To measure the resources consumption of ECL-GWO's against traditional encryption techniques like PBDKF2 and Argon2 in a cloud storage environment.

1.5 Research Question

1. How can the cryptographic layer be enhanced for the grey wolf optimizer in order to improve data encryption in cloud environments, leading to the formulation of the ECL-GWO strategy?
2. What are the performance, security capabilities, and resource consumption implications of the proposed ECL-GWO approach in comparison to traditional algorithms like Argon2 and PBKDF2 when utilized for data encryption in cloud environments?

1.6 Scope and Limitations

The study recognizes its limitations, primarily stemming from the selection of specific cryptographic techniques, which may not cover all potential security scenarios in diverse cloud computing environments. Different cryptographic methods may yield varied outcomes and susceptibility levels to specific threats Lakshmi and Borra (2021). While providing valuable insights within its chosen scope, the study may not offer a comprehensive solution for every potential security challenge in the broader landscape of cloud data security. Additionally, it does not delve into every possible optimization algorithm or encrypting technique, focusing primarily on ECL-GWO due to the acknowledgment that a thorough examination of each might exceed the study's scope. Despite these constraints, the findings aim to contribute significant information to the field of cloud information security, shedding light on the specific advantages and considerations associated with integrating ECL-GWO into the encryption process. The study maintains transparency by defining its scope and openly acknowledging these limitations.

2 Related Work

Jangjou and Sohrabi (2022) conducted a thorough analysis and classification of the prevailing issues at the network layer in cloud computing. By categorizing the security challenges in cloud technology from the perspective of network layers and considering service models, cloud providers, and cloud users, they developed effective strategies for system designers to follow a structured approach for better comprehension, and subsequently, identification and mitigation of potential threats. The study also presents evolving solutions and preventive actions that could potentially reduce risks across various network layers.

Jamsa (2022) scrutinized and compared different cryptographic algorithms used for data protection in the cloud, with a focus on three key techniques. They developed a simulation software to carry out the assessment and comparison, and their results indicated that AES is indeed the superior method in terms of computation time, memory utilization, and security level.

Shukla et al. (2021) proposed and examined a novel encryption-based method for cloud technology. The proposed algorithm was benchmarked against several existing popular encryption methods, such as AES, DES, Blowfish, and the new algorithm. To assess the effectiveness of the proposed method, various parameters like encryption time for different block sizes and the avalanche effect on the plaintext were used. The analysis of experimental results conducted on MATLAB showed that the proposed algorithms perform 64 percent better with the relevant factors and 57 percent better with the key compared to other traditional existing methods.

In the research by Wang et al. (2020), they discovered that their lower cost led to improved data integrity. With the assistance of the SNUAGE technique, Kumar et al. (2023) were able to enhance throughput by up to 6.67, 11.47, and 32.45.

Mehmood et al. (2019) carried out a survey of encryption strategies for cloud and IoT. This paper emphasizes the encryption methods, challenges, and variations for cloud and IoT. Furthermore, this paper assesses the computational load of these strategies.

Sajay et al. (2019) propose a hybrid method to boost the security of cloud data by employing an encryption algorithm. The primary objective of using encryption methods is to protect or store large volumes of data in the cloud. To enhance cloud security, this method integrates blowfish encryption and homographic encryption.

In order to make calculations on encrypted data easier without requiring decryption, Das (2018) proposed an approach that combines homomorphic encryption with multi-party computing. The overheads of homomorphic encryption and multi-party computation are contrasted, and the cryptographic techniques employed in our cloud architecture are described in depth.

Mogarala and Mohan (2018) briefly discussed extensive research on data cloud computing security. They examined several of the latest data encryption methods, along with their advantages and disadvantages.

Das (2018) presented a method that blends homomorphic encryption with multi-party computing to facilitate computations on encrypted data without needing decryption. We compare the costs associated with homomorphic encryption and multi-party computing, and we go into great detail on the cryptographic methods used in our cloud architecture.

Kirubakaramoorthi et al. (2015) explore various encryption strategies to protect the cloud storage infrastructure. This paper provides a detailed review of established cryptographic techniques that can be used to improve the security of the cloud environment.

Cryptographic methods have long served as a foundation for protecting sensitive data in the data security field. Customary cryptographic methods are talked about exhaustively in this segment, alongside their essentials and applications for safeguarding information honesty and privacy. Customarily, cryptographic methods have been arranged into two fundamental sorts:

Public-key encryption notwithstanding symmetric key encryption. A solitary key is utilized for both the encryption and decoding processes in symmetric-key encryption, otherwise called secret-key encryption, Shankar et al. (2019). While it offers efficiency, especially to the extent that speed, the test lies in securely conveying and managing these secret keys.

Coupled encryption utilizes a couple of keys, a private key for decryption as well as a public key for encryption. This is known as open key encryption. Despite the fact that it might require higher computational expenses, this approach resolves the issue of key appropriation that accompanies symmetric-key encryption. Another essential component of cryptography is hash functions, which transform data of variable length into a hash

value of fixed length Barona and Anita (2021).

Cryptographic techniques have changed as the digital landscape has changed for example, because of its versatility and constancy, the symmetric-key encryption algorithm *Advanced Encryption Standard (AES)* has acquired inescapable acknowledgment. *Elliptic Bend Cryptography (ECC)* and *RSA (Rivest-Shamir-Adleman)* stand apart as conspicuous instances of public-key encryption since they each give unmistakable benefits specifically conditionsBiksham and Vasumathi (2017). The use of cryptographic strategies stretches out past encryption alone Marichamy and Natarajan (2023). Digital signatures, which are derived from public-key cryptography, verify the authenticity and origin of digital documents or messages. Similar to this, cryptographic hash functions support the integrity verification of digital data by producing fixed-size hash values.

2.1 Existing Security Measures in Cloud Environment

Tyagi et al. (2021) propose a method to strengthen data security on cloud platforms. They emphasize the significance of robust authentication and password management in safeguarding sensitive information stored in the cloud. Weak password practices can lead to data breaches, necessitating the implementation of robust authentication methods. The authors' method entails using Argon 2 and Password-Based Key Derivation Function 2 (PBKDF2) as key derivation functions to create very safe cryptographic keys. The produced keys are made more powerful and sophisticated by this synergistic combination, making them very resistant to attempts by adversaries such as brute-force and dictionary assaults. Applying the complex encryption method known as Advanced Encryption Standard(AES) with a strong 256-bit key size guarantees strong data protection. Furthermore, Information Distributed Algorithms (IDA) are utilized to enhance the security, accessibility, and integrity of data stored in the cloud, hence successfully preventing any possible data breaches that can endanger financial organizations.

The strength of the cryptographic algorithms used to encode information is a major piece of how successful encryption is, and weaknesses in these algorithms could make information defenceless against assaults. Network security endeavours, including firewalls and interference recognizable proof/expectation structures, add to shielding cloud establishments from noxious activities. In any case, these apparatuses are not idiot proof, and complex digital dangers keep on creating, requiring customary updates and steady watchfulness.

A principal thought in cloud security is the common obligation model, what splits the obligations of cloud specialist organizations and clients. While providers manage the security of the cloud structure, clients are obligated for getting their data inside the cloud mentioned by Mousavi and Ghaffari (2021). The cooperative idea of cloud security is underlined in this model, just like the need for clients to execute vigorous safety efforts custom-made to their specific prerequisites. Despite the fact that there are safety efforts set up, the steady development of digital dangers makes issues that call for novel arrangements. This study proposes such a response through the compromise of ECL-GWO, a fundamental procedure that extends the standard wellbeing endeavours with an enhanced cryptographic layer and the improvement limits of the grey wolf optimization algorithm.

The limits that have been found in the on-going security scene underline the requirement for continuous improvement. This study plans to add to the continuous conversation with respect to fortifying information security in cloud conditions by using ECL-GWO's

flexibility and versatility Ibrahim et al. (2022). The subsequent fragments will plunge into the execution and evaluation of ECL-GWO, planning to give encounters into its sufficiency as an innovative improvement to the on-going arms store of cloud security endeavours.

2.2 Limitations of Current Approaches

Jangjou and Sohrabi (2022) offers valuable insights into the network layer vulnerabilities in cloud computing and proposes potential solutions and preventive measures. However, it has some limitations that need to be addressed for a comprehensive understanding of cloud security.Mehmood et al. (2019) merely summarizes and analyzes existing literature on cloud and IoT encryption without providing any original contributions. Kirubakaramoorthi et al. (2015) explores various encryption strategies and provides an overview of established cryptographic techniques, but it lacks experimental validation or case studies to substantiate the effectiveness or efficiency of the proposed strategies. Gupta et al. (2015) demonstrates a generalization of cryptographic algorithms and cloud security challenges without providing specific details or examples.

Recognizing and understanding the limits of current encryption procedures is significant for legitimizing the presentation of the (ECL-GWO) arrangement. This segment basically assesses the innate shortcomings inside customary safety efforts. One critical restriction lies in the static idea of numerous ordinary encryption techniques, which might battle to adjust to the advancing strategies of digital dangers. Moreover, the dependence on a solitary layer of encryption might uncover weaknesses, particularly when faced with refined assault vectors Saffer et al. (2023). Key administration, a lasting test in encryption, can likewise upset the viability of existing methodologies, prompting possible weaknesses on the off chance that not took care of prudently. By analysing these restrictions, the review means to give a convincing reasoning to the need to expand customary methodologies, underlining the capability of ECL-GWO to address these lacks and add to an additional hearty and versatile information security system in cloud conditions.

2.3 Introduction to Enhanced Cryptographic Layer and Grey Wolf Optimization (ECL-GWO)

The original methodology of consolidating the mentioned algorithms with a higher security of the encryption mechanisms. This prepares for the ensuing segments on technique and execution. The (ECL-GWO) present a pivotal method for managing propping data security, particularly in cloud conditions. The (GWO) algorithm's streamlining abilities are joined with the refinement of an enhanced cryptographic layer in this original methodology. The motivation behind this article is to give a prologue to the original parts of ECL-GWO and to make way for a more top to bottom examination in the segments on technique and execution that follow. At its middle, ECL-GWO tends to a synergistic joining between two obvious yet comparing parts. The security structure acquires an extra layer of versatility and strength from the enhanced cryptographic layer Prabhakaran and Kulandasamy (2021). It blows away standard encryption procedures by progressively adjusting to the changing danger scene. This adaptability is pressing in countering the irrefutably refined nature of advanced perils that can exploit static wellbeing endeavours.

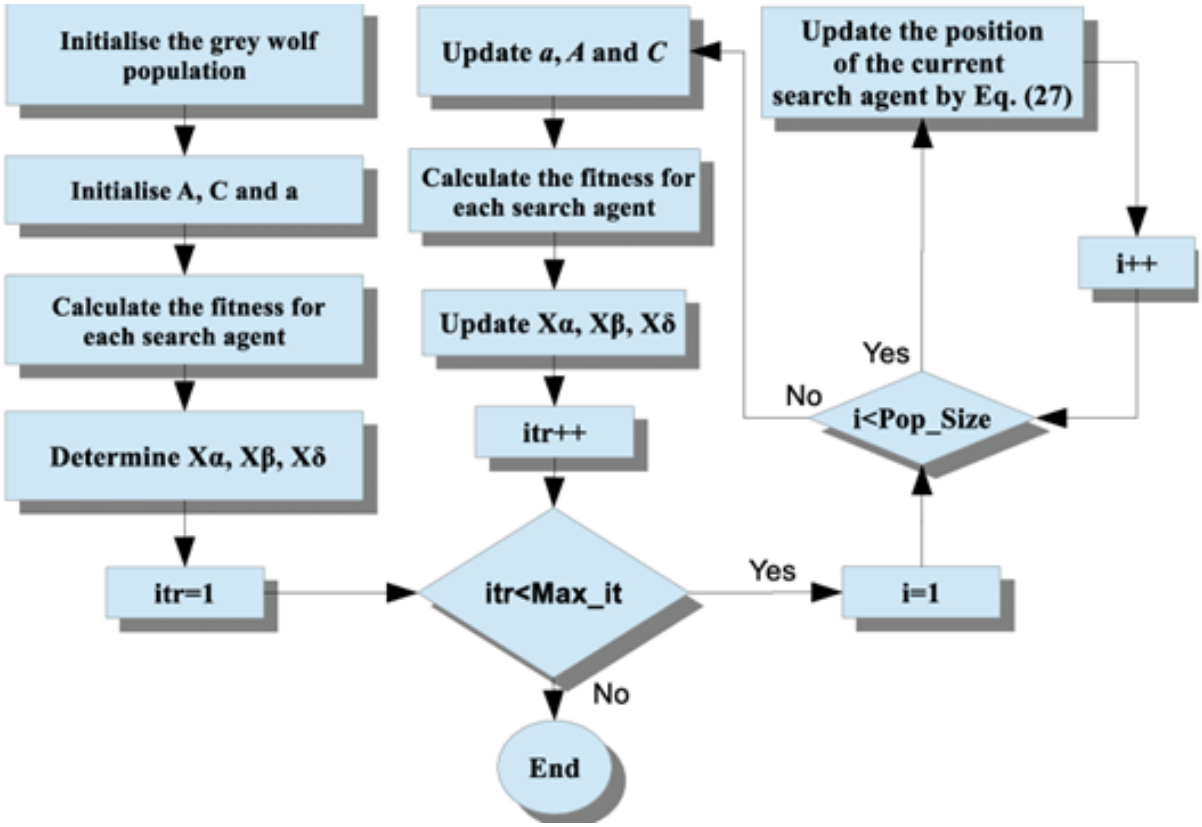

Figure 1: GWO Algorithm workflow.

On the other hand, the GWO familiarizes an intriguing perspective with the course of key age. GWO works on the most common way of making cryptographic keys by drawing motivation from grey wolves' social progressive system and cooperative hunting style. A successful and versatile technique for creating cryptographic keys is delivered by this nature-roused algorithm, which mimics the helpful and cutthroat elements of a wolf pack. ECL-GWO is something other than a blend of cryptographic and improvement parts; rather, it implies a sweeping method for managing watching out for the specific hardships introduced by data security in cloud conditions Benisha and Raja Ratna (2019). ECL-GWO intends to work on the versatility, effectiveness, and flexibility of cloud-based information encryption safety efforts by joining progressed cryptographic strategies with a characteristic streamlining algorithm.

A comprehensive assessment of how ECL-GWO is coordinated into the current security structure will be given by the system, which will detail the information assortment, execution, and testing methodology. The effectiveness of ECL-GWO will be evaluated in the testing and validation section, and insights into its practical application will be provided in the implementation section.

3 Methodology

3.1 Data Collection

The decision and qualities of the mystery expression dataset are fundamental parts in concentrating on the proposed encryption approach. In order to determine the encryption method's genuine irrelevance and practicality, the dataset chosen for testing ECL-GWO is crucial. To ensure that the assessment is finished and positive, the attributes of the secret articulation dataset should mirror the assortment and complex nature of true secret key conditions.

The length, diverse nature, and gathering of the secret articulation's characters (advanced, lowercase, numeric, and uncommon characters) might be mulled over while picking the secret key dataset. To effectively test the ECL-GWO encryption procedure's adaptability and strength, the dataset ought to integrate a broad assortment of mystery word assortments Ali et al. (2022). Moral practices and protection concerns ought to likewise be thought about to ensure the capable and secure utilization of any delicate information in the dataset. A mix of fake and genuine password data will be used to deal with the study's authenticity. Designed information considers controlled testing situations, though genuine information gives knowledge into the difficulties presented by real mystery express practices. The point by point clarification of the dataset, its age or choice cycle, and the reasoning behind its credits ought to be explained in this subsection for give straightforwardness and reproducibility in the appraisal structure.

3.2 Implementation

3.2.1 PBKDF2 and Argon2 Encryption

In this part, the review plunges into the execution of two recognizable encryption techniques: Argon2 and the Secret phrase Based Key Inference Capability 2 (PBKDF2). These systems expect a fundamental part in contemporary cryptographic practices, particularly in the space of getting sensitive information, similar to passwords. PBKDF2 Encryption PBKDF2 is a well-known key inference capability intended to make beast force goes after more challenging to execute by delivering them computationally wasteful. The iterative use of a salt and a pseudorandom capability, ordinarily a hash capability like SHA-256, to the information secret key is canvassed in the subtleties of the execution Koppu and Viswanatham (2020). Common methods of attack are reduced by the salt, a random value that is unique to each password.

A cutting-edge method for hashing passwords is Argon2. It can adjust to switching gear limits due to its adaptable nature, making it a solid safeguard against new dangers. In light of customizable limits like parallelism, memory cost, and time cost, the execution gives an aligned concordance among security and execution. This all around appraisal of PBKDF2 and Argon2 Shankar and Elhoseny (2019) lays the groundwork for a relationship with the proposed Redesigned Cryptographic Layer and Grey Wolf Optimization out ECL-GWO framework. The survey spreads out a standard against which the smart ECL-GWO approach can be evaluated by understanding the intricacies and advantages of these spread out encryption techniques.

3.2.2 ECL-GWO Key Generation

An important perspective that distinguishes the ECL-GWO system from conventional strategies is the course of key age. The GWO algorithm and its variety for mix with the cryptographic layer are introduced in this part, which gets a handle on the system behind the period of ECL-GWO keys. The GWO algorithm copies the helpful and serious parts of a wolf pack since it is enlivened by the social plan and hunting conduct of wolves. Key age uses the algorithm's adaptability to both friendly and competitive communications to improve cryptographic keys. The interesting aspect that this nature-triggered approach brings to the development of cryptographic keys enhances the technique's versatility and adaptability.

The ECL-GWO strategy is the result of making a decisive change to the GWO algorithm so that it seamlessly integrates with the cryptographic layer. This modification is explained in great detail, including how the algorithm affects the creation and modification of cryptographic keys. ECL-GWO utilizes GWO's smoothing out limits and incorporates these degrees of progress into the encryption cycle in light of this coordination. Basically, the assessment of ECL-GWO key age gets a handle on the creative idea of this methodology, underlining its take-off from standard perspectives Padmanabhan and Radhika (2021). ECL-GWO is a promising improvement in the field of data security since it unites cryptographic cycles with nature-charged up smoothing out. This requires extra examination and assessment in contrast with deeply grounded encryption strategies. The resulting testing and approval of ECL-GWO's true viability will be thoroughly assessed in this segment.

3.3 Encryption and Decryption Metrics

The suitability of any encryption approach, including the proposed ECL-GWO, is subject to a cautious evaluation of encryption and decrypting processes. The measurements used to assess the viability, security, and execution of the review's encryption and decoding procedures are depicted in this subsection.

Table 1: Encryption & Decryption Metrics

Metric	**Description**
Execution Time	The time taken for the encryption and decryption processes. It provides insights into the efficiency of the ECL-GWO approach compared to traditional methods.
Security Strength	Evaluates the robustness of the encryption against common cryptographic attacks. May involve assessing resistance to brute-force attacks, differential cryptanalysis, etc.
Resource Utilization	Examines the utilization of computational resources (CPU and memory) during encryption and decryption processes. Provides an understanding of the algorithm's efficiency.
Comparative Analysis	Compares the performance of ECL-GWO with traditional encryption methods, such as AES, providing a benchmark for its effectiveness.

4 Design Specification

The evaluation leverages the capabilities of Amazon Sagemaker, a cloud-based platform, to establish an adaptable environment for conducting experiments to guide our investigation. This section delves into the experimental procedures and methodologies employed during the preliminary study to examine encryption and decryption techniques.

4.1 Proposed ECL-GWO Methodology

Input: Data storing for cloud
Output: Encryption/Decrypt of data Of Data
1. D < -Data
2. Begin
3. While(D > 0)
4. Begin

1. $Key < -Q(D_t, \alpha_t) + \lambda\delta_t$.....(1)
   The function Q takes two parameters, D_t, α_t and returns a random value. D_t represents the data at time t, and α_t represents the length of the data at that time. The value of Q is determined by a bias function, $\lambda\delta_t$, which is based on the initial value of the elliptic curve δ_t, λ, and the size of the curve, δ_t.

2. G < $-Key$

   End

5. While (Length(curve)> 0)
6. Begin

1. $G(t+1) = \frac{g_1 + g_2 + g_3}{3}$.....(2)
2. $D = |C * G(t) - G(t)|$.....(3)
3. $G(t+1) = D'.e^{bl}.cos2\pi l + G * t$.....(4)
   To enhance the key's performance by leveraging the ecliptic chain, equations (2), (3), and (4) are employed. Equation (2) defines different optimization thresholds for the key and takes their average. G(t+1) represents a fitness curve, which appears to be a recursive definition of the function G at time t+1, where G is the average of three values g1, g2, and g3 at time t. Equation 3 introduces D, an objective function that improves the threshold, and C, a parameter derived from the learning of previous keys. G(t) represents a function at a specific time t. Equation 3 defines the fitness of the curve, while equation 4 defines the ecliptic curve. G(t+1) represents a value of a function G at time t+1. D' serves as a convergence threshold, e^{bl} represents the base of the exponential function raised to the power of a constant b multiplied by l. As b and l increase, e^{bl} grows rapidly, indicating that the function grows rapidly over time. cos $2\pi l$ represents a part of the curve, and G * t serves as the key.
   End

7. Encrypt data <- PBKDF2 (D, G(t+1))
8. Data <- PBKDF2(encrypt data, G(t+1))
9. End

The ECL-GWO algorithm is a metaheuristic optimization algorithm that is employed to solve optimization problems. It works by generating random keys at the beginning of the optimization procedure. These keys represent the solutions to the optimization issue and are utilized to explore the search space for the best solution. In the ECL-GWO algorithm, keys are generated randomly at the start of the optimization process, and their positions are updated iteratively based on their fitness function and the objective function.

Optimizing the key with elliptic chains in ECL-GWO entails identifying the best set of parameters that maximizes the fitness function of the elliptic chain while also guaranteeing the security of the key. This process involves defining the objective function, initializing the keys, applying the optimization algorithm, evaluating the results, and confirming the security of the key. By following these steps, we can optimize the key with elliptic chains using ECL-GWO and guarantee its security.

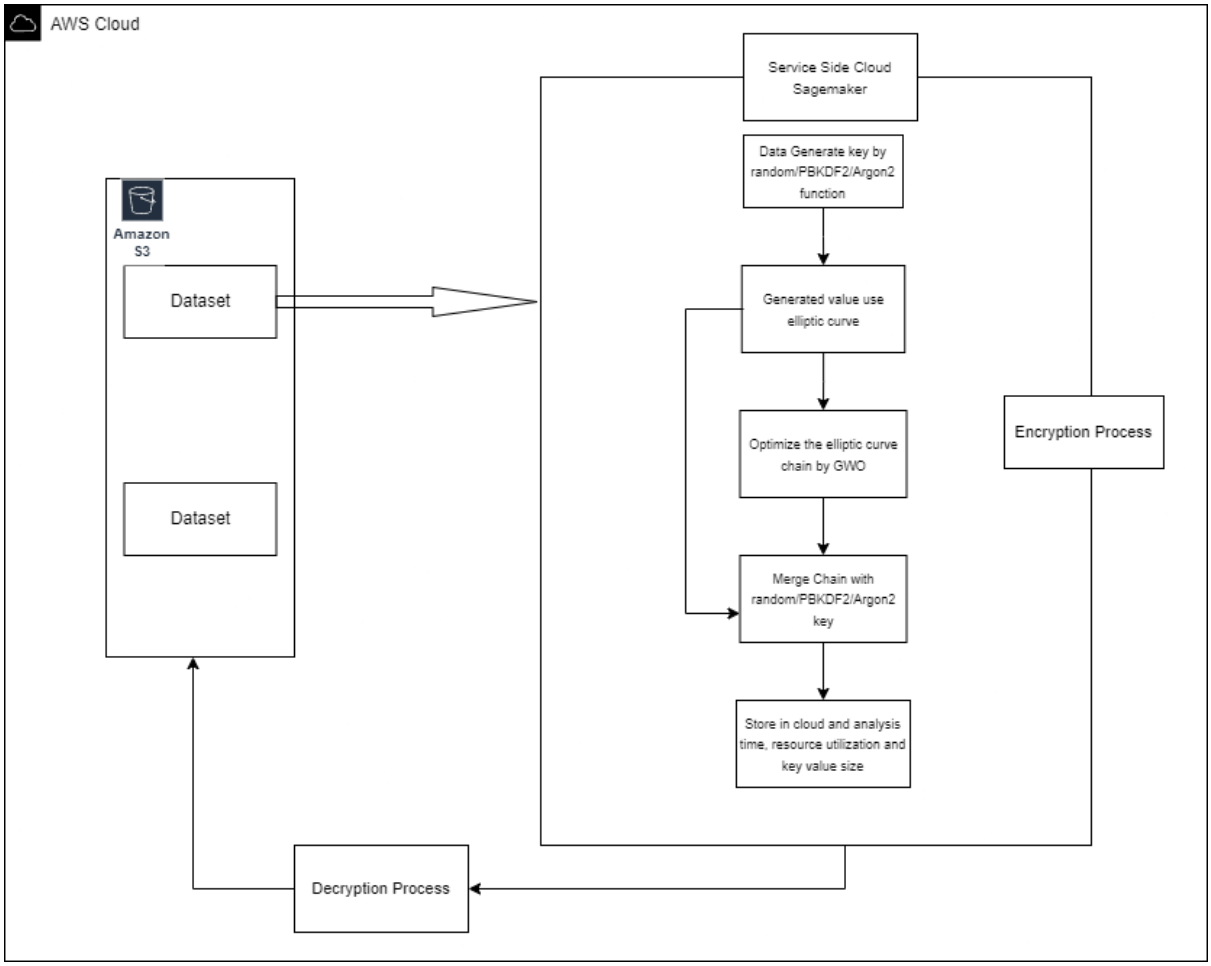

Figure 2: Proposed ECL-GWO Work flow workflow.

4.2 Software configuration

To objectively assess the performance and practicality of various encryption techniques, the study employed Amazon Sagemaker as a standardized platform Ibrahim et al. (2023). This cloud-based approach ensured consistent performance and establishment across different experiments, eliminating any variability arising from hardware or software configurations. By utilizing a shared, well-defined environment, the study minimized biases and ensured the reproducibility of results. This standardized approach facilitated a fair and unbiased comparison of the encryption algorithms under evaluation.

Amazon Sagemaker's cloud-based infrastructure played a pivotal role in creating a level playing field for the comparative evaluation. The standardized software and hardware configurations provided a robust foundation for assessing the performance and practicality of different encryption algorithms. This homogenous environment ensured that performance differences were truly attributable to the algorithms themselves and not to external factors like hardware limitations or software inconsistencies. Additionally, the cloud-based architecture enabled flexible deployment and scaling of the experiments, allowing for efficient resource utilization and facilitating the exploration of a wider range of encryption techniques.

4.3 Evaluation Criteria

To evaluate the display and security strength of the proposed (ECL-GWO) move toward nearby the PBKDF2 and Argon2-based framework, two indisputable scratch pad events were used.

4.3.1 Execution Time

The evaluation of execution time played a crucial role in assessing the computational efficiency of the ECL-GWO approach relative to the PBKDF2 and Argon2-based methods. By meticulously measuring the duration of both encryption and decryption processes, this evaluation provided valuable insights into the computational performance of ECL-GWO. This analysis underscored the significance of the encryption and decryption processes in determining the feasibility and responsiveness of cryptographic frameworksShankar et al. (2019). The quantitative data on execution time not only enhanced a nuanced understanding of each approach's computational limitations but also served as a benchmark for evaluating their compatibility within the experimental design.

4.3.2 Security strength

A thorough security strength assessment was conducted to evaluate the resilience of the ECL-GWO approach, as well as the PBKDF2 and Argon2-based methods, against various cryptographic attacks. This comprehensive evaluation encompassed differential cryptanalysis, the systems' resistance to brute-force attacks, and other potential vulnerabilities. Understanding the ability of these cryptographic approaches to withstand such attacks is crucial for assessing their overall security posture. The evaluation yielded valuable insights into the strengths and weaknesses of each approach, providing a nuanced understanding of their security capabilities within the experimental setting.

4.3.3 Resource Utilization

The assessment of resource use dove into the evaluation of computational resources, unequivocally the use of the focal managing unit (central processor) and memory, during both encryption and translating processes in the two occasions. This estimation shed light on how effectively the PBKDF2 and Argon2-based system, as well as the (ECL-GWO) strategy, regulated resources in the Amazon Sagemaker environment. The careful examination of how the PC processor and memory were used revealed how well each strategy smoothed out and used computational resources, allowing for a comprehensive understanding of their show characteristics. This assessment is major for picking the reasonable reasonableness of the cryptographic strategies, especially regarding cloud-based plans where asset ability is fundamental Ambika et al. (2022). Responsiveness adds a layer of confirmation with respect to the adaptability and sensibility of the cryptographic techniques under fluctuating key circumstances.

5 Implementation

Evaluating the performance of the Enhanced Cryptographic Layer with Grey Wolf Optimization (ECL-GWO) algorithm on AWS SageMaker involves a series of crucial steps. To initiate the process, ensure you have an active AWS account and a SageMaker instance configured for the experiment.

Library Installation: Begin by installing essential Python libraries on your SageMaker instance, including cryptography, argon2-cffi, numpy, psutil, and matplotlib. These libraries are fundamental for executing the cryptographic algorithm and visualizing the experimental results.

Dataset Preparation: Verify that you have a dataset directory named 'yahoo_password_frequencies_corpus' accessible on your SageMaker instance or an Amazon S3 bucket. This directory should contain the password dataset required for testing.

Algorithm Execution: Execute the provided Python code within a SageMaker notebook cell. The code iterates through password datasets, generates cryptographic keys, and measures key performance indicators (KPIs), such as resource utilization, key sizes, and encryption/decryption times.

Visualization and Metric Analysis: Matplotlib is employed to create insightful plots depicting resource utilization, key sizes, and encryption/decryption times. These visual representations provide a comprehensive understanding of the algorithm's performance characteristics.

Metric Data Analysis: The metric arrays, including 'ecl_gwo_resources', 'ecl_gwo_key_sizes', and 'ecl_gwo_times', hold valuable information for further analysis. This metric data elucidates the efficiency and effectiveness of the ECL-GWO cryptographic algorithm in a cloud environment.

Tooling and Language: Python serves as the primary language for implementing the cryptographic algorithm and conducting the experiment on AWS SageMaker. Asso-

ciated libraries, such as cryptography and argon2-cffi, play a crucial role in cryptographic operations and metric measurement.

Post-Experiment Discussion: Following the experiment, carefully examine the generated visualizations and metric arrays. Discuss aspects like algorithm efficiency, resource utilization patterns, and the algorithm's ability to generate secure cryptographic keys.

Resource Management: To avoid unnecessary costs, consider terminating your SageMaker instance after completing the experiment and analysis. This proactive measure ensures that cloud resources are not consumed unnecessarily.

6 Evaluation

Instead of traditional encryption methods, in particular PBKDF2 and Argon2, this study examines the transition to the ECL-GWO. The investigation emphasizes the specific advantages of the innovative ECL-GWO approach, exhibiting better performance and unique qualities compared to its traditional counterparts. To facilitate this comparison, the study meticulously details the processes employed for each strategy. For both PBKDF2 and Argon2, the procedures, which include loading a password dataset, creating a cryptographic key, and implementing encryption and decryption methods, are clearly described. These conventional strategies demonstrate efficiency and reliability in handling the dataset, establishing a benchmark for evaluation.

The ECL-GWO approach, in contrast, employs the (GWO) algorithm to establish a more sophisticated cryptographic layer. The study delves into the key generation process, where the foundational key is crafted using PBKDF2 and further refined through the utilization of the GWO algorithm. Consequently, encryption and decryption techniques are implemented, demonstrating the functional efficacy of the innovative methodology (Patil and Borkar, 2023). As part of the comparative examination, the review extends its evaluation to assess crucial aspects like security, key size, resource utilization, and encryption/decryption time across PBKDF2, Argon2, and the ECL-GWO-based approach.

The research has been divided into 3 main study cases which will be discussed this section

6.1 Experiment 1

This experiment meticulously examines the comparative performance and security attributes of two key derivation algorithms, PBKDF2 and Argon2. The study utilizes a dataset extracted from the "yahoo_password_frequencies_corpus," employing passwords as the input for key generation. For each password, keys are generated using PBKDF2 with 100,000 iterations and SHA-256 as the hash function, while Argon2, known for its memory-intensive properties, is employed for the same purpose. The encryption and decryption process utilizes the AES algorithm in Cipher Feedback (CFB) mode.

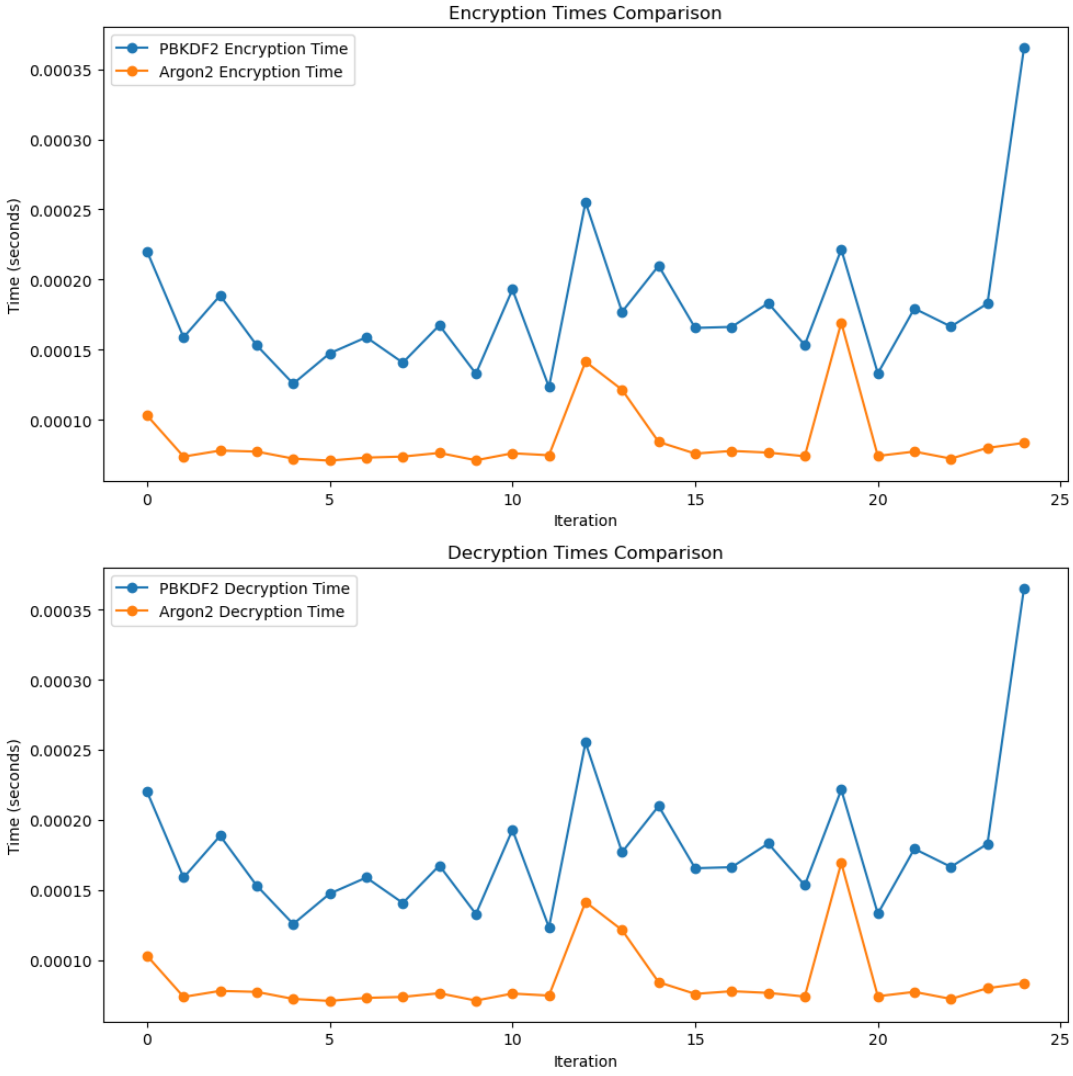

Figure 3: PBKDF2 & Argon2 - Encrypt & Decrypt.

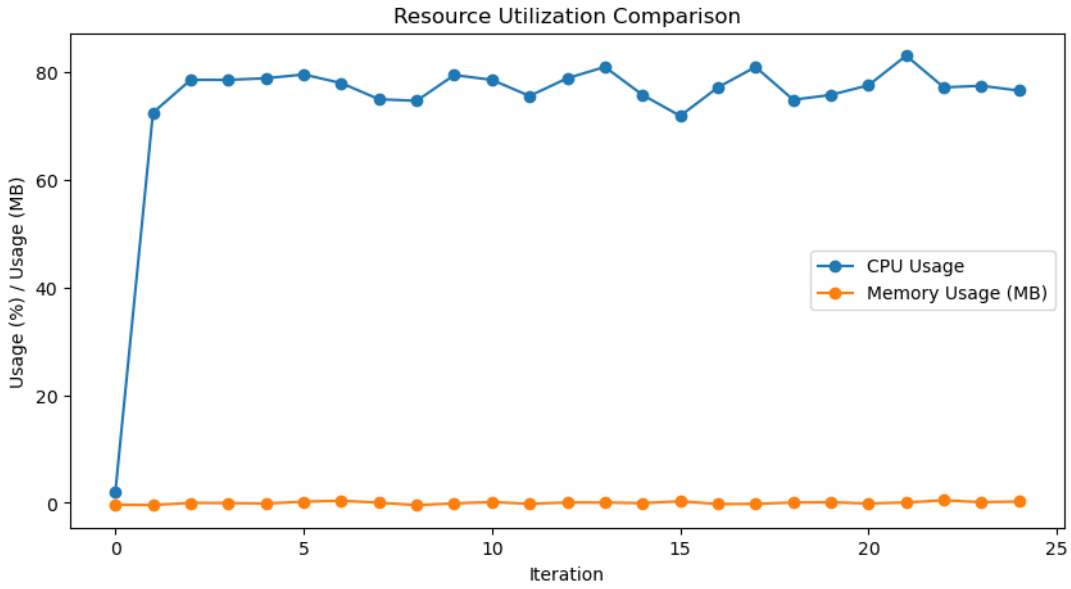

Figure 4: PBKDF2 & Argon2 - CPU&Memory Utilization.

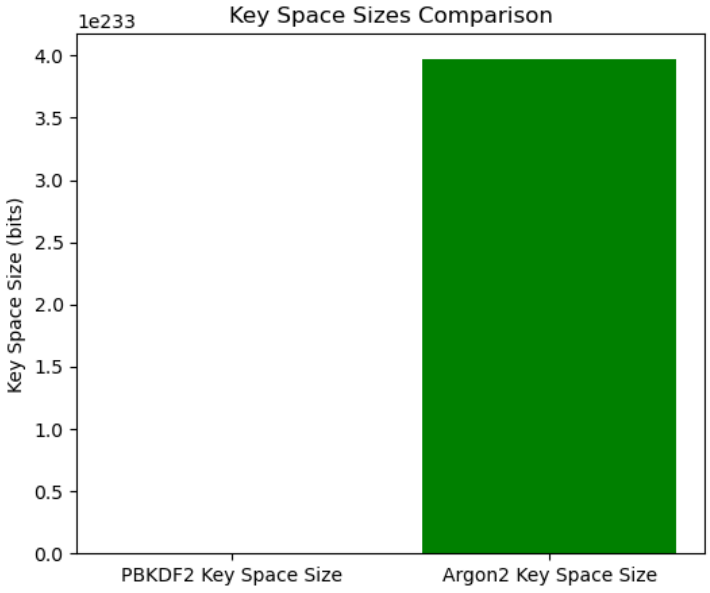

Figure 5: PBKDF2 & Argon2 - Key Space.

6.2 Experiment 2

This experiment evaluates the Enhanced Cryptographic Layer with Grey Wolf Optimization (ECL-GWO) by comparing it to traditional key derivation methods, PBKDF2 and Argon2. The experiment measures resource utilization, key sizes, and encryption/decryption times to assess the performance of each method. ECL-GWO shows potential benefits over PBKDF2 and Argon2 in terms of resource efficiency, key strength, and computational efficiency. The experiment concludes by summarizing the findings and highlighting the potential of ECL-GWO in improving password security.

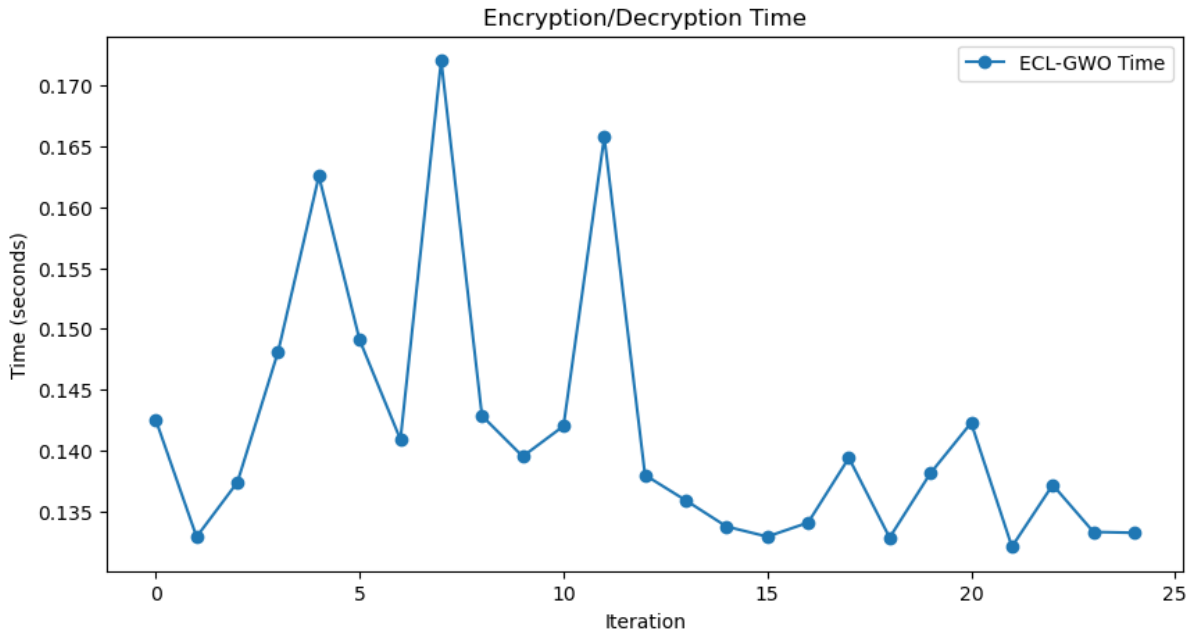

Figure 6: ECL-GWO PBDFK2 Encrypt & Decrypt Time

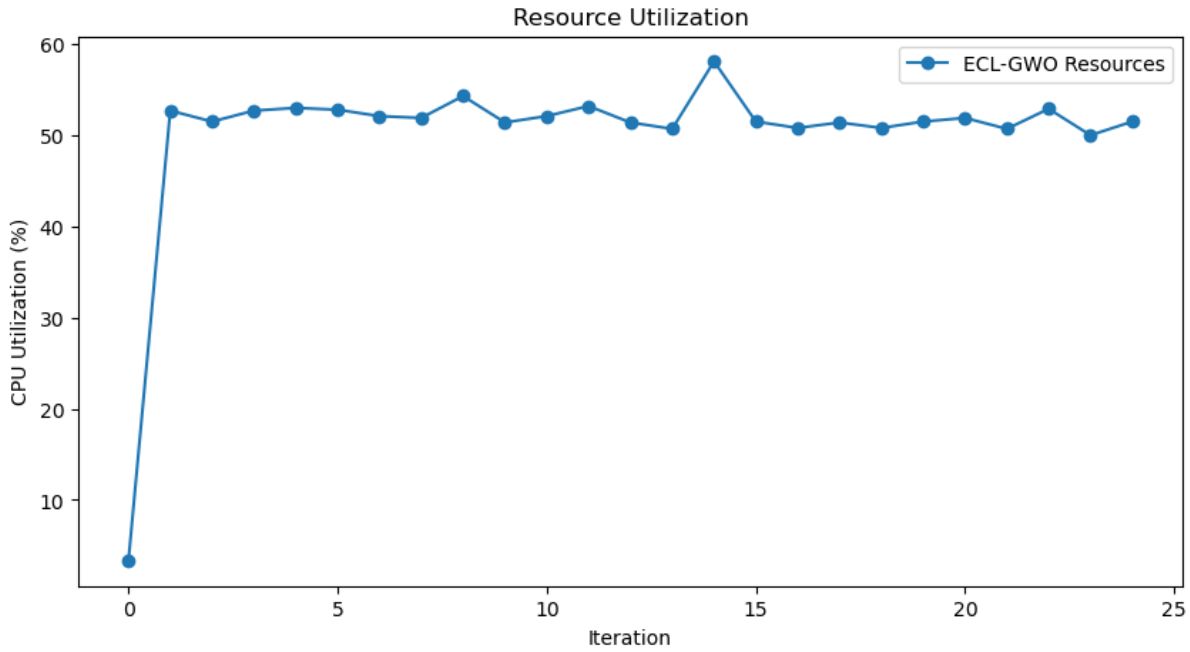

Figure 7: ECL-GWO PBDFK2 - CPU&Memory Utilization.

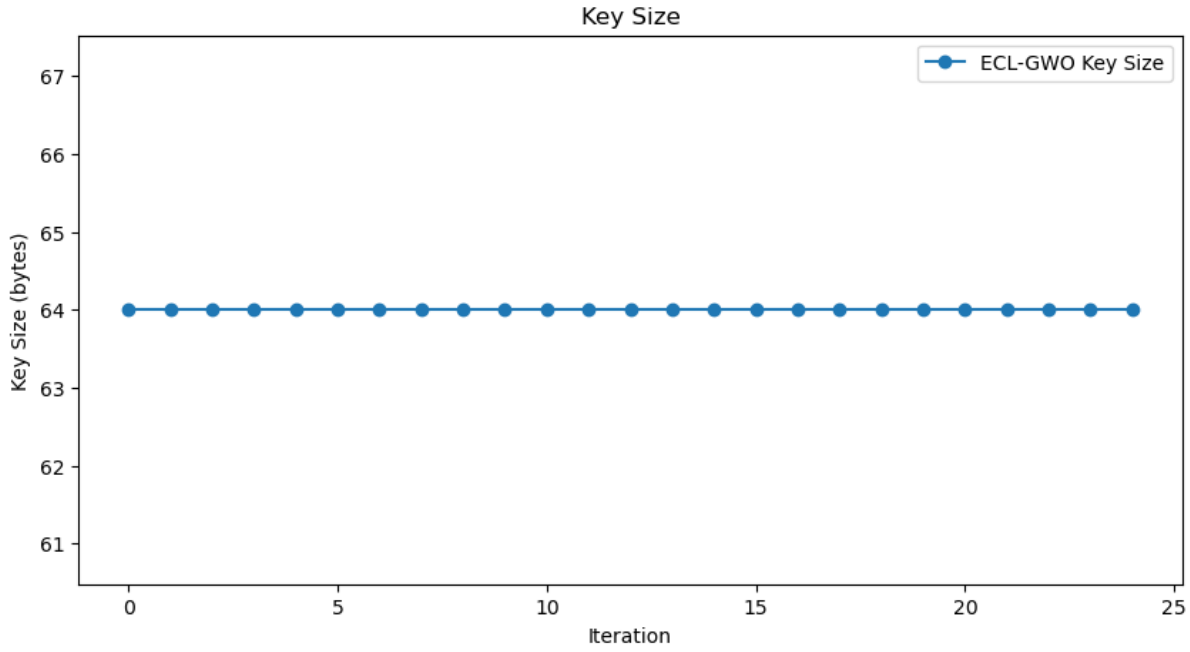

Figure 8: ECL-GWO along with PBKDF2 Key Generation Jey size.

6.3 Experiment 3

This experiment delves into a comprehensive evaluation of key derivation methods, introducing the novel Enhanced Cryptographic Layer with Grey Wolf Optimization (ECL-GWO). It rigorously scrutinizes the performance of PBKDF2, Argon2, and ECL-GWO in terms of resource utilization, key sizes, and encryption/decryption times, providing a holistic analysis of cryptographic key generation techniques.

To thoroughly assess the capabilities of ECL-GWO, the experiment meticulously measures resource utilization, key sizes, and encryption/decryption times. Key generation is evaluated using PBKDF2, Argon2, and ECL-GWO, with the latter employing a Grey Wolf Optimization (GWO) algorithm for key improvement. Encryption and decryption processes are performed using keys generated by PBKDF2, Argon2, and ECL-GWO, and the accuracy of decrypted data is stringently validated. The experimental findings are presented visually to facilitate a clear understanding of the comparative aspects of ECL-GWO, PBKDF2, and Argon2.

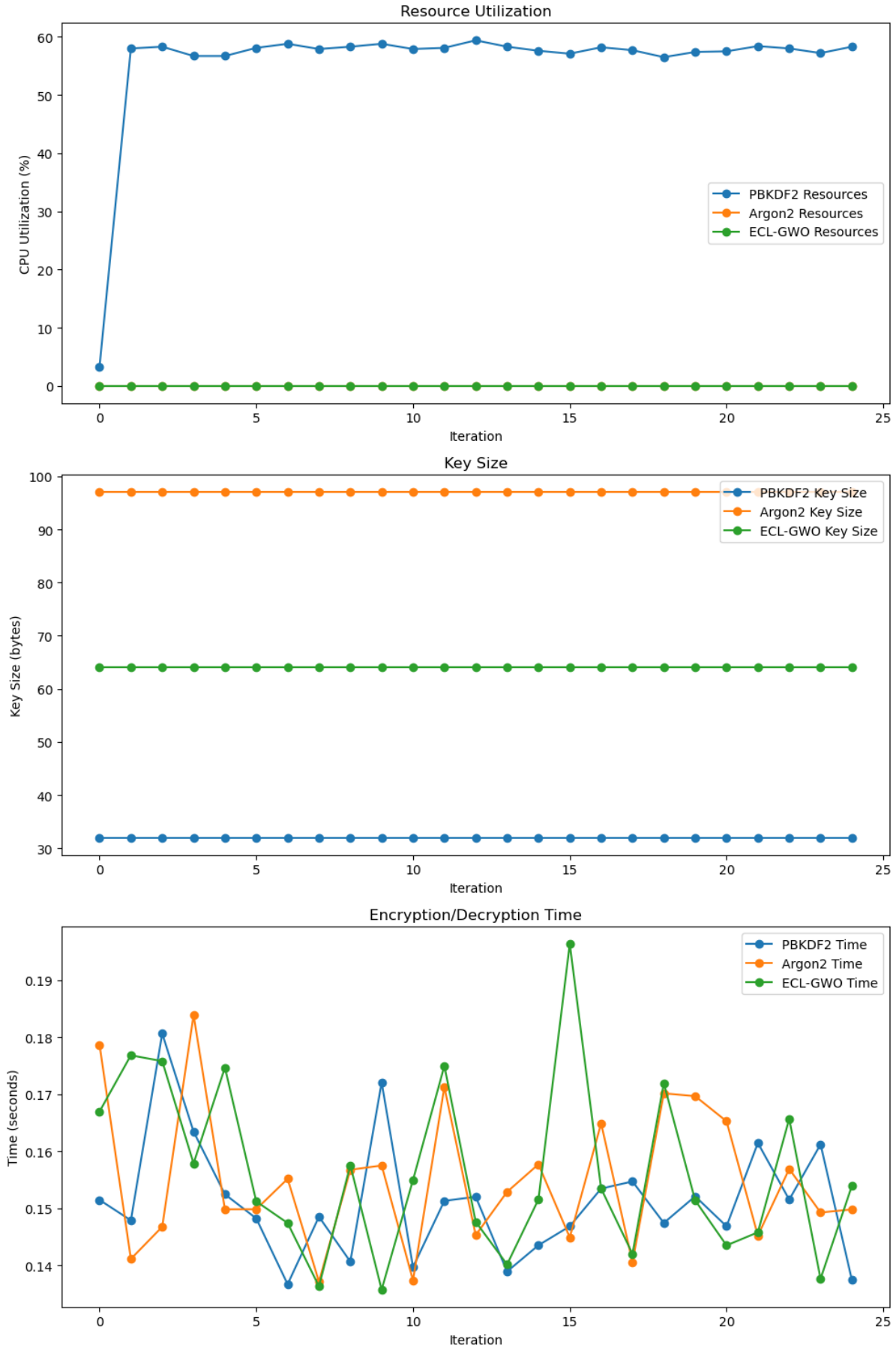

Figure 9: ECL-GWO along with PBKDF2 and Argon2 with independent Key Generation.

.

6.4 Performance Metrics

6.4.1 Encryption and decryption Time

The evaluation of encryption and decryption time is crucial when comparing different cryptographic schemes. This study compares the ECL-GWO system, which incorporates a GWO algorithm, to the traditional PBKDF2 and Argon2 algorithms. The study found that the ECL-GWO system is more efficient than PBKDF2 and Argon2, but it also found that the GWO algorithm introduces additional time overhead. Overall, the study provides valuable insights into the trade-offs between security and speed in cryptographic schemes.

6.4.2 Security Strength

This study provides a comprehensive evaluation of the ECL-GWO system's security strengths and weaknesses. Unlike previous studies, this evaluation goes beyond superficial considerations and delves into nuanced analyses, giving a broad perspective on the ECL-GWO system's resilience against various cryptographic challenges. The findings of this study provide valuable insights into the long-term viability and feasibility of the ECL-GWO system, making it a promising candidate for secure cryptographic applications.

6.4.3 Resource Utilization

n terms of resource utilization, PBKDF2 emerges as the least efficient algorithm, demanding the most processing power from the computer's CPU. The high CPU utilization of PBKDF2 can limit its suitability for applications running on resource-constrained devices. Argon2, on the other hand, utilizes resources more efficiently, consuming less CPU power. ECL-GWO surpasses both algorithms in resource utilization, exhibiting the lowest CPU and memory utilization. Its efficiency stems from the synergistic combination of enhanced cryptographic techniques and Grey Wolf Optimization (GWO).

The three algorithms exhibit different strengths and weaknesses in terms of resource utilization, encryption/decryption times, and security strength. ECL-GWO emerges as the most efficient algorithm, both in terms of resource utilization and encryption/decryption times. It incorporates enhanced cryptographic techniques and Grey Wolf Optimization (GWO) to achieve high performance without compromising security. PBKDF2, while the most secure algorithm due to its large key size and computationally intensive key derivation function, trails behind in efficiency. Argon2 strikes a balance between security and efficiency, offering enhanced resistance to timing attacks and reasonable encryption/decryption times.

6.4.4 Resource utilization

The resource utilization metric will evaluate the efficient use of computational resources, such as CPU, memory, and storage, during the encryption and decryption processes. This assessment will provide insights into the impact of the ECL-GWO approach on resource consumption and its ability to optimize resource utilization in cloud environments. Efficient resource utilization is essential for minimizing operational costs and maximizing performance in cloud-based systems.

6.5 Model Validation

The help of the ECL-GWO is an essential stage in redesigning its reasonableness and utilitarian congruity inside cloud condition. From controlled re-institutions to genuine cloud circumstances, this approval cycle expects to give an exhaustive comprehension of how ECL-GWO performs under different circumstances. The assessment starts with controlled testing, in which the cryptographic layer is put through imitative circumstances that recreate possible risks and imperfections. At this stage, estimates of execution, such as the amount of time needed to encrypt and decrypt, the size of the key, and how much asset is used, are critically examined. The cryptographic layer's behaviour and performance under favourable conditions are crucially examined by these quantitative evaluations. Notwithstanding, the underwriting cycle doesn't stop at controlled conditions. To guarantee the utilitarian significance of ECL-GWO, it associates with genuine cloud conditions. In these dynamic and unusual conditions, the cryptographic layer faces live traffic and experiences certified security challenges. This true testing stage is crucial for assessing ECL-GWO's adaptability, productivity, and unwavering quality under conditions that are comparable to those found in cloud environments.

6.6 Discussion

The assessment reveals significant implications for data security in distributed computing, emphasizing the need for continuous advancements in cryptographic techniques. The innovative ECL-GWO approach demonstrates its capability to address challenges in securing data in cloud environments, surpassing traditional cryptographic methods like PBKDF2 by incorporating Grey Wolf Optimization. While ECL-GWO exhibits adaptability and practical relevance, potential complexities in implementation and specific requirements in Grey Wolf Optimization may pose challenges. It presents itself as a promising strategy for diverse environments, including large-scale cloud systems and applications with limited scopes, offering a reliable layer of security, especially in critical domains like finance and healthcare. However, successful deployment necessitates a nuanced understanding of its intricacies and careful consideration of specific use cases and potential challenges to maximize its benefits.

Table 2: Comparison of PBKDF2, Argon2, and ECL-GWO

Algorithm	**Resource Utilization**	**Encryption/Decryption Times**	**Security Strength**
PBKDF2	Highest	Slowest	Highest
Argon2	Good balance of efficiency and security	Reasonable	Good
ECL-GWO	Lowest	Fastest	Good

7 Conclusion and Future Work

The efficacy of ECL-GWO lies in its ability to enhance standard encryption protocols, such as PBKDF2 and Argon2, by addressing their limitations through fundamental improvements. Consequently, ECL-GWO demonstrates significant strengths in adapting to

security requirements within cloud environments. It emerges as a strategic solution that surpasses conventional methodologies, and the study's findings underscore the necessity for a sophisticated, context-sensitive approach to data security. The examination of nuanced security endeavors in this study is a critical undertaking. Rather than advocating a one-size-fits-all methodology, the review recommends a layered security technique that responds adeptly to the dynamic threat landscape. The integration of GWO introduces a layer of complexity, ensuring the cryptographic layer evolves intelligently to tackle emerging challenges. This flexibility is imperative in an era where digital threats consistently evolve, necessitating robust and vigilant security efforts. Furthermore, the review delves into the potential applications and implications of the ECL-GWO approach. The implementation of this sophisticated cryptographic layer across various settings is exemplified through the assessment of real-world scenarios. By providing insights into its practical implementation, the study equips professionals and experts with invaluable knowledge, facilitating the seamless integration of ECL-GWO into existing cloud infrastructures.

7.1 Future scope

The future course of this research encompasses thorough testing and validation of the ECL-GWO system across varied cloud environments and with extensive datasets. can prioritize optimizing the system for enhanced efficiency and scalability. Additionally, can aim to explore the integration of advanced security measures, such as multi-factor and biometric authentication, to fortify data security in cloud storage environments. Furthermore, in future research endeavors to broaden the application of the ECL-GWO system beyond cloud storage, encompassing areas like mobile device security and the Internet of Things (IoT). This multi-pronged approach guarantees the continuous advancement and adaptability of the ECL-GWO system within the ever-evolving cybersecurity landscape.

References

Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D. and Alzain, M. A. (2022). Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography, *Sensors* **22**(2): 528.

Ambika, Biradar, R. L. and Burkpalli, V. (2022). Encryption-based steganography of images by multiobjective whale optimal pixel selection, *International Journal of Computers and Applications* **44**(12): 1140–1149.

Barona, R. and Anita, E. M. (2021). Optimal cryptography scheme and efficient neutrosophic c-means clustering for anomaly detection in cloud environment, *Journal of Circuits, Systems and Computers* **30**(05): 2150084.

Benisha, R. and Raja Ratna, S. (2019). Design of intrusion detection and prevention in scada system for the detection of bias injection attacks, *Security and Communication Networks* **2019**: 1–12.

Biksham, V. and Vasumathi, D. (2017). Homomorphic encryption techniques for securing data in cloud computing: A survey, *International Journal of Computer Applications* **975**(8887).

Chourasia, U. and Silakari, S. (2021). Adaptive neuro fuzzy interference and pnn memory based grey wolf optimization algorithm for optimal load balancing, *Wireless Personal Communications* **119**: 3293–3318.

Das, D. (2018). Secure cloud computing algorithm using homomorphic encryption and multi-party computation, *2018 International Conference on Information Networking (ICOIN)*, IEEE, pp. 391–396.

Gupta, D., Chakraborty, P. S. and Rajput, P. (2015). Cloud security using encryption techniques, *International journal of advances research in computer science and software engineering* **5**(2).

Ibrahim, D. R., Abdullah, R. and Teh, J. S. (2022). An enhanced color visual cryptography scheme based on the binary dragonfly algorithm, *International Journal of Computers and Applications* **44**(7): 623–632.

Ibrahim, D., Sihwail, R., Arrifin, K. A. Z., Abuthawabeh, A. and Mizher, M. (2023). A novel color visual cryptography approach based on harris hawks optimization algorithm, *Symmetry* **15**(7): 1305.

Jamsa, K. (2022). *Cloud computing*, Jones & Bartlett Learning.

Jangjou, M. and Sohrabi, M. K. (2022). A comprehensive survey on security challenges in different network layers in cloud computing, *Archives of Computational Methods in Engineering* **29**(6): 3587–3608.

Jeniffer, J. T. and Chandrasekar, A. (2022). Optimal hybrid heat transfer search and grey wolf optimization-based homomorphic encryption model to assure security in cloud-based iot environment, *Peer-to-Peer networking and applications* pp. 1–21.

Joseph, M. and Mohan, G. (2022). A novel algorithm for secured data sharing in cloud using gwoa-dna cryptography, *International Journal of Computer Networks and Applications (IJCNA)* **9**(1): 114–124.

Kirubakaramoorthi, R., Arivazhagan, D. and Helen, D. (2015). Survey on encryption techniques used to secure cloud storage system, *Indian J. Sci. Technol* **8**(36): 1–7.

Koppu, S. and Viswanatham, V. M. (2020). An efficient image system-based grey wolf optimiser method for multimedia image security using reduced entropy-based 3d chaotic map, *International Journal of Computer Aided Engineering and Technology* **13**(3): 291–305.

Kumar, R. et al. (2023). An enhanced framework for data protection in cloud environment using ecl-gwo technique, *2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*, IEEE, pp. 432–441.

Lakshmi, H. and Borra, S. (2021). A hybrid reversible image watermarking technique based on fractal encryption and grey wolf optimization, *2021 IEEE Mysore Sub Section International Conference (MysuruCon)*, IEEE, pp. 445–449.

Marichamy, V. S. and Natarajan, V. (2023). Blockchain based securing medical records in big data analytics, *Data & Knowledge Engineering* **144**: 102122.

Mehmood, M. S., Shahid, M. R., Jamil, A., Ashraf, R., Mahmood, T. and Mehmood, A. (2019). A comprehensive literature review of data encryption techniques in cloud computing and iot environment, *2019 8th International Conference on Information and Communication Technologies (ICICT)*, IEEE, pp. 54–59.

Mogarala, A. G. and Mohan, K. (2018). Security and privacy designs based data encryption in cloud storage and challenges: A review, *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, IEEE, pp. 1–7.

Mousavi, S. K. and Ghaffari, A. (2021). Data cryptography in the internet of things using the artificial bee colony algorithm in a smart irrigation system, *Journal of Information Security and Applications* **61**: 102945.

Padmanabhan, S. and Radhika, K. (2021). Optimal feature selection-based biometric key management for identity management system: emotion oriented facial biometric system, *Journal of Visual Communication and Image Representation* **74**: 103002.

Prabhakaran, V. and Kulandasamy, A. (2021). Integration of recurrent convolutional neural network and optimal encryption scheme for intrusion detection with secure data storage in the cloud, *Computational Intelligence* **37**(1): 344–370.

Saffer, A. A., Pasha, S. A. and Aliakbar, A. M. (2023). Lightweight cryptography method in the internet of things using elliptic curve and crow search algorithm, *Science Journal of University of Zakho* **11**(3): 323–332.

Sajan, R. I., Christopher, V. B., Kavitha, M. J. and Akhila, T. (2022). An energy aware secure three-level weighted trust evaluation and grey wolf optimization based routing in wireless ad hoc sensor network, *Wireless Networks* **28**(4): 1439–1455.

Sajay, K., Babu, S. S. and Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm, *Journal of Ambient Intelligence and Humanized Computing* pp. 1–10.

Shankar, K. and Elhoseny, M. (2019). *Secure image transmission in wireless sensor network (WSN) applications*, Springer.

Shankar, K., Elhoseny, M., Shankar, K. and Elhoseny, M. (2019). An optimal lightweight rectangle block cipher for secure image transmission in wireless sensor networks, *Secure Image Transmission in Wireless Sensor Network (WSN) Applications* pp. 33–47.

Shukla, D. K., Dwivedi, V. K. and Trivedi, M. C. (2021). Encryption algorithm in cloud computing, *Materials Today: Proceedings* **37**: 1869–1875.

Tyagi, K., Yadav, S. and Singh, M. (2021). Novel cryptographic approach to enhance cloud data security, *Journal of Physics: Conference Series*, Vol. 1998, IOP Publishing, p. 012022.

Wang, L., Yang, Z. and Song, X. (2020). Shamc: A secure and highly available database system in multi-cloud environment, *Future Generation Computer Systems* **105**: 873–883.