International Journal of Advanced Technology and Engineering Exploration, Vol 11(117)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2023.10101660

Research Article

Enhancing cloud storage security through blockchain-integrated access control and optimized cryptographic techniques

R.S.Kanakasabapathi[1*] and J.E.Judith[2]
Research Scholar, Department of Computer Applications, Nooral Islam centre for Higher Education, Tamil Nadu, 629180, India[1]
Associate Professor, Department of Computer Science and Engineering, Noorul Islam centre for Higher Education, Tamil Nadu, 629180, India[2]

Received: 24-May-2023; Revised: 13-August-2024; Accepted: 16-August-2024

Abstract
In the ever-changing landscape of technological innovation and the growing security concerns associated with cloud storage, this research focuses on the critical topic of improving cloud record security. The study introduces a paradigm for access control that integrates with the Ethereum blockchain. To enhance security, an improved salp swarm optimization (ISSO) technique is employed to generate the crucial random numbers required for secret key generation. Additionally, the research utilizes two more encryption algorithms: the Paillier federated multi-layer perceptron (PF-MLP) model and the homomorphic encryption standard (HES), to further protect the original health tweet dataset's privacy. The study evaluates the security constraints and efficacy of various encryption methods, guiding the selection of the strongest framework to safeguard the health tweets dataset. The ISSO technique streamlines key pair generation, making it more challenging for potential attackers to access the original data. The proposed encryption-decryption method demonstrates superior speed, with encryption times of 800 ms and 900 ms, respectively, outperforming both the Rivest–Shamir–Adleman (RSA) algorithm and elliptic curve cryptography (ECC). Additionally, the approach surpasses ECC and RSA in upload and download speeds, with times of 4 ms and 6 ms, respectively. With a processing time of 1500 ms, the proposed method significantly outperforms previous approaches, showcasing its efficiency and superiority in cryptographic operations. This work combines access control, blockchain technology, and advanced cryptographic techniques to address pressing security issues related to cloud storage. By enhancing data safety and confidentiality, the integrated framework represents a significant advancement in the security of data outsourced to cloud platforms.

Keywords
Data security, Salp swarm optimization, Homomorphic encryption standard, Cloud computing, Paillier federated learning, Ethereum blockchain.

1.Introduction
The rapid growth of cloud systems has significantly transformed the way data is stored and accessed. However, it has also raised serious concerns about data security. As businesses increasingly rely on cloud systems to store sensitive information, ensuring data security and protection has become paramount [1]. Traditional methods of safeguarding information have struggled to address the new challenges associated with securing data in the cloud. This paper presents a novel approach to enhancing data security in cloud systems, combining improved salp swarm optimization (ISSO), Paillier federated multi-layer perceptron (PF-MLP), and homomorphic encryption standard (HES).

Cloud computing has garnered significant interest from academics due to its collaborative efficiency, reliability, competence, cost-effectiveness, and extensive file-storage capabilities. It also relies on virtualization, which involves interconnecting multiple computers and servers to enable information sharing [2, 3]. The key challenges in implementing this technology are related to data availability, integrity, and accessibility. However, protecting cloud-based information is an exceptionally difficult and time-consuming process. Consequently, several experts are developing new, less resource-intensive cryptographic methods and other protective measures. Cryptographic methods are becoming crucial because they substantially guarantee data privacy, secrecy, and

*Author for correspondence

confidentiality [4, 5]. These methods enable safe and efficient retrieval of data from cloud storage [6].

Cloud computing, a kind of emerging virtualization technology, provides a variety of on-demand solutions at reasonable pricing [7]. The primary objective of cloud computing is to provide fast, easy backup computing and data processing assistance [7, 8]. There are dangers and hazards in the cloud computing environment, despite the fact that the computer age has successfully interacted with cloud computing services. One of the most important parts of cloud data security is a cryptosystem, which may be used in conjunction with other measures to make cloud computing safer.

Confidentiality is maintained throughout the transmission of communications or data. It also details how the sender's message is transformed into a "cypher text," a secret code that can be read only by the specified recipient's computer [7]. Furthermore, the cloud computing criteria may offer certain workable data service practices, such as the utilization of processing resources for peak performance in software, telecommunications aid, social networking sites, and online applications [8]. In addition, cloud technology in computer servers is very helpful for consumers to gather and retrieve their data remotely at any moment without any extra burden. However, cloud data storage has major security issues. Therefore, cloud data centers must implement certain protocols to ensure the integrity and security of data on its journey to the cloud. "Cloud security" is an umbrella term for many strategies that ensure the integrity of data stored in the cloud in the face of persistent attacks.

Elastica Q2 2015 and cloud security alliance (CSA) investigate how to build security into a cloud app that allows for administration, deception, and recovery. In addition, the International Organization for Standardization (ISO) recognizes data security concerns that may be associated with cloud computing's crucial security measures for a workable and trustworthy innovation in technology (*Figure 1*).

This exemplifies how cloud computing safeguards are crucial. Information and application outsourcing in the cloud shifts control away from the end user and towards the service provider. Therefore, confidence relies on the modelling approach and cloud provider.

Current security methods either have poor security or require a lot of time to encrypt and decrypt the data [1–3]. Due to the lengthier procedure, more frequent modifications, power consumption, and network latency are required [3].

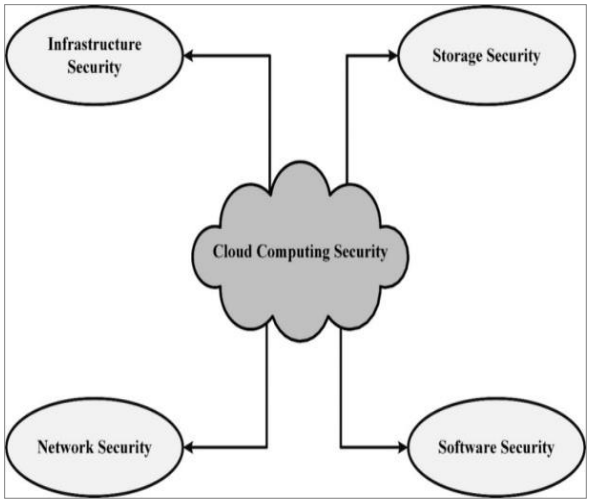

Figure 1 Cloud security

Customers should have access to security measures, given the importance of these to the cloud computing paradigm and the efficient sharing of resources and information. Therefore, it is the responsibility of cloud service providers to provide not just efficiency in terms of energy use, network latency, and time needed, but also safety and dependability. Cloud infrastructure security cannot be effectively assessed using existing methodologies [5].

In cloud computing, a cost-effective method is essential since it streamlines operations and provides immediate access to computing resources. For better data security in the cloud, the structure should use encryption and decryption that require less network authority, time, and delay to complete. However, cloud architecture has problems with connection, scalability, and sharing resources among several users.

Cloud infrastructure is vulnerable to a variety of problems as a network that relies on network connections (including embedded channels, grid computing, and so on), with security being the primary area of concern. Security concerns would slow down the rapid adoption of cloud computing. Connecting cloud computing services raises the difficulty of maintaining this information's security and privacy to stop its abuse or misuse. Cloud-stored information is especially vulnerable to this issue. One of the biggest threats to the safety of cloud computing is network security, which includes protection from both external and internal attack [6–8]. There are several systems in place to ensure the safety of data transfer across

network connections, but cryptography remains the most effective one. Ciphertext is the result of a cryptographic text conversion specifically, it is a tool for securely transmitting content by ensuring that only the intended recipient might discover it.

In the 1950s and 1960s, researchers employed perceptron's, which consisted of an input layer, an output layer, and a hidden layer [9]. To get to the output nodes—where the classification decisions are made—the eigenvectors from the input nodes must first pass through the hidden nodes on their way there. It was Rosenblatt who initiated the first perceptron's [10]. Rosenblatt's single-layer perceptron has a major flaw in that it can't deal with somewhat complex characteristics.

Homomorphic encryption (HE) has made it possible to employ encrypted messages in the field of deep learning. Encryption techniques were initially proposed in 1978 by Rivest et al. [11]. HE is a kind of encryption in which the encrypted message may be decrypted by applying a specified arithmetic operation to it. The result of applying the same operation to the encrypted message as to the plain text is the same in both cases [12].

In contrast to the Rivest–Shamir–Adleman algorithm (RSA) and EI Gamal analysis tools that enable multiplicative homomorphisms, there are presently no truly HE algorithms available. While this is a significant advancement in homomorphic cryptography, its high cost and complex mathematical model prevent its practical use at the present time. Thereafter, researchers [13] presented a sweeping homomorphic encryption (SWHE) scheme. Only operations of low polynomial order are important to this sort of encryption. Mojisola et al. [14] suggested security and privacy as the two biggest concerns of the cloud.

Infiltration possibilities into cloud infrastructure are many and expanding. The companies that host these services in the cloud are concerned about data security and privacy. The supplier must take precautions to protect its own infrastructure as well as its customers' software and data by implementing protective procedures and standards. User aversion to cloud computing is mostly driven by security fears, as reported by Shinde and Taur [15]. It is important to evaluate the security processes of cloud providers since many suppliers are unwilling to make their transportation networks public and because monitoring and building a cloud security region is a difficult task.

Advanced security, as stated by Sangeetha et al. [16], necessitates an efficient storage technique. Since breaking in half is necessary for effective warehousing, the kind of damage usually depends on the availability of storage space and the price of repair. No matter how secretive the standoff is, it may be split using a process that creates numerous divisions of the same size. Security flaws in cloud storage might result in financial losses and reputational harm if the framework is intended for widespread usage. These worries are what are making this novel strategy so popular. Client data saved in the cloud may include crucial information. Because of this, it is not preferable for unauthorised parties to breach data security. Users should take care while saving files in the cloud and should encrypt all data before uploading it [17].

Previous studies have highlighted several significant obstacles to cloud data security. Firstly, traditional encryption techniques can be highly computationally intensive, making them unsuitable for real-time processing and cloud-based data analytics [10–14]. Secondly, coordinating cloud-based access control and authentication becomes challenging when numerous users are involved [11–15]. Finally, ensuring data privacy while allowing encrypted data to be processed collaboratively remains a significant challenge [13–17].

HE algorithms are on the rise and are increasingly being used in a wide variety of application settings to ensure data security [12, 13]. Complex optimisation issues are often approached with the help of multi-objective optimisation algorithms like ant colony optimisation (ACO), firefly algorithm (FA), whale optimisation (WO), particle swarm optimisation (PSO), bee colony optimisation (BCO), and so on. The current methods suffer from significant limitations, including increased computational complexity, excessive time consumption, reduced speed, higher error rates, and a less secure environment [13–17].

The goal of this paper is to enhance cloud data security in multiple ways. First, it introduces a method for optimizing the efficient production of key pairs in cloud systems using the ISSO technique. Second, it incorporates the PF-MLP model to strengthen protections against unauthorized access to private information. Third, the study implements the principles of HES to enable secure collaborative data

processing in cloud environments. Additionally, the paper conducts a comprehensive analysis to evaluate the efficiency and security limitations of the proposed strategy, providing robust data to support its validity in practical cloud settings.

Furthermore, this study offers actionable insights and recommendations, guiding businesses in their efforts to enhance data security in the cloud. The principal contributions of this paper lie in its innovative fusion of ISSO, PF-MLP, and HES approaches, which improve the efficiency of key generation, strengthen access control, and increase data privacy for cloud-stored information. Empirical assessments validate these contributions, making this study a valuable resource for those aiming to bolster cloud-based data security. To further enhance cloud data security, the recommended technique includes delivering an optimized encryption mechanism.
The main contributions of this study are as follows:

- Employ two new encryption specifications, HES and PF-MLP, to enhance the security of the health tweet dataset.
- Develop a secure cloud storage architecture with restricted access using the blockchain. This architecture combines the Ethereum blockchain with the ciphertext-policy attribute-based encryption (CP-ABE) method to achieve fine-grained access management for remote storage without the need for a trusted feature source.
- Utilize Ethereum's smart contract framework to store crucial data on the blockchain system, thereby achieving decentralization in the cloud storage architecture.
- The security of sensitive health data is protected using a federated learning (FL) method based on HE.
- A hybrid ISSO technique is employed to generate the key pair needed by the encryption strategy to enhance the safety of the tweet health dataset while reducing computation time.
- To ensure the security of cloud data, an ISSO-based optimisation method is employed to identify the optimum model for creating secret keys.
- During the assessment, the various kinds of performance assessments were validated and contrasted to demonstrate that the ISSO-HES process functions properly.

The following sections of this article are organized as follows: Sections 1 and 2 discuss and evaluate traditional meta-heuristic and biologically influenced optimization schemes. Section 3 covers the proposed methodology, including the PF-MLP model and the HES. In Section 4, different assessment metrics are employed to evaluate the performance outcomes of the proposed and conventional cryptographic strategies. It also covers the results implications. Finally, Section 6 summarizes the entire paper and outlines future work.

2.Related works

Related work is discussed in this section, along with the methodological interventions, advantages, and disadvantages.

Wang et al. [18] presented a method for securely outsourcing optimization computations. Using cloud computing for linear programming (LP) simulations, they distinguished between private client-owned LP variables and public cloud-based LP solutions. They developed privacy-preserving algorithms to protect sensitive data, ensuring accuracy through LP's core duality postulate. Extensive security analysis demonstrated the method's immediate applicability.

George and Jayashree [19] discussed a novel method to access management and authentication for safe data sharing in cloud storage that is built on the Ethereum blockchain. This technique addressed concerns about stakeholder trust and improves data integrity verification. By using data rules for access control and integrating the interplanetary file system (IPFS) and Ethereum blockchain, the framework lowers costs and improves throughput in the cloud model by distributing secret keys. Results show that the suggested blockchain-assisted technique is successful, with high user detection rates, accurate keyword search on ciphertext, and efficient response.

Sheeba et al. [20] examined how the internet of things (IoT) and blockchain security may be used to change how data-driven businesses make decisions. The difficulties with security, transparency, and complexity in business financial transactions are addressed by the suggested digital hash data encryption (DHDE) method. DHDE provides a complete solution for protecting company transactions in the dynamic world of IoT and Blockchain integration by encrypting transaction data, and improving the security of embedded system users and blockchain.

Panda et al. [21] investigated the privacy and security issues that arise when using electronic health record (EHR) systems in cloud settings. It draws attention to the vulnerabilities in the manner in which cloud storage handles private medical data as well as the shortcomings in the method trusted third parties (TTP)

handle authentication and data security. Blockchain technology is a strong solution that leverages distributed ledger characteristics, hash values, and extensive access control mechanisms to provide tamper-proof, trustworthy, and secure EHR data transfer.

Dule and Roopashree [22] used blockchain technology inside the Ethereum ecosystem to create a framework model that solves privacy problems in cloud-based picture data sharing. By using a duplication method and stakeholder agreement, the suggested model attempts to achieve optimal time complexity and security while guaranteeing effective access control and cryptography techniques. The evaluation of the novel Ethereum-based ecosystem for protecting and optimizing image data privacy shows notable reductions in data repositioning time, retrieval time, operational cost, delay, and faster algorithm execution time when compared to traditional cloud-built distributed systems.

Antony and Samiappan [23] addressed security and storage issues by introducing a revolutionary method of secure data transfer utilizing an IPFS-based blockchain with access control and authentication. The suggested concept goes through eight stages to provide strong access control and storage capabilities, involving entities like smart contracts, holders of data, data requesters, blockchains, and IPFS. High detection rates, little communication overhead, and superior privacy rates are demonstrated by the findings, which confirm how well the IPFS-based blockchain and access control system operate together to provide safe transactions inside the blockchain network.

Sucharitha et al. [24] presented an innovative method for improving cloud security communication: Blockchain-assisted ciphertext policy decentralized attribute-based encryption (BA-CP-DABE). The indestructibility of blockchain combined with CP-DABE for key generation and data access management guarantees ciphertext secrecy and permits fine-grained search over encrypted data. Using comprehensive numerical tests, the suggested approach proves its effectiveness in creating key and trapdoor structures and in safely finding encrypted data on the blockchain.

Mahajan and Reddy [25] addressed issues with security, scalability, and computing efficiency in Healthcare 4.0 by putting forth a unique method for processing gene profile data securely. The proposed Healthcare 4.0 architecture offers a centralized, secure framework for the interchange and storage of gene data by utilizing blockchain technology and lightweight cryptography. The model is a potential option for the safe processing of microarray gene expression data since it shows improved computing efficiency and security, including notable reductions in encryption and decryption times and strong protection against many threat types.

Almasian and Shafieinejad [26] presented an attribute-based encryption (ABE) and blockchain-based safe cloud file sharing system. By utilizing ABE for user anonymity and smart contracts on blockchain, the decentralized system allows data owners to safely exchange files with users and facilitates quick access revocation. The study certifies the security of the scheme by formal verification, and assessment findings show that it is scalable with acceptable performance for a significant number of users, indicating that it is a promising option for safe and effective cloud file sharing.

Kallapu et al. [27] presented an attribute-aware encryption architecture backed by blockchain technology to improve cloud communication security. The suggested technique secures access to encrypted data using keyword searches on the blockchain and enables data owners to set fine-grained search permissions using ABE [28]. It offers a viable method for secure communication over the cloud in real-time and contains a functional comparison of ABE algorithms along with numerical tests testing key generation, trapdoor construction, and keyword retrieval capabilities.

To further protect sensitive information during cloud operations, Sajay et al. [29] proposed a hybrid encryption technique. To safeguard the system's verifiability, privacy, usability, data retrieval, and integrity, it proposes to use new encryption criteria. For this purpose, we merged the functional needs and procedures of two different encryption schemes, namely HE and blowfish encryption approaches, to improve the overarching security of cloud-based operations. It also investigated the efficiency and efficacy of several encryption techniques, including the Hellman algorithm, digital signatures, the message digest 5 (MD5) blow-fish algorithm, and the advanced encryption standard (AES). This research concludes that HE strategies are superior to other methods for protecting sensitive information during cloud-based operations. There are, however, major problems with its processing speed, key generation complexity, and memory consumption. Zhao et al. [30] highlighted the

necessity for a HE approaches to enhance cloud computing security due to its rapid growth and popularity for storing apps and data. Despite cloud computing's benefits like scalability and virtualization, traditional security measures are inadequate, prompting active research into novel security components that manage encrypted data efficiently. However, computational challenges remain a significant drawback.

Das [31] developed a secure cloud computing algorithm using HE and multi-party computation to encode and protect data without decryption. This approach employs optimal asymmetric encryption padding (OAEP) and a hybrid encryption on RSA, ensuring data confidentiality and integrity. Despite the advantages in privacy and security, the method is costly and computationally intensive.

These works highlight the complex trade-offs in cloud-based data security and privacy. Researchers are balancing computational efficiency and communication overhead, with significant contributions in FL and privacy-preserving collaborative machine learning. Techniques like "vFedSec" optimize secure aggregation in vertical FL without sacrificing data privacy. However, challenges in scaling and reducing communication costs persist, demonstrating the intricate balance required between data privacy, efficiency, and collaborative learning in federated settings [32–37].

3.Proposed method

This research anticipates that utilizing an intelligent optimization-based encryption approach enhances the privacy, security, and confidentiality of cloud storage. The proposed modeling approach is depicted in *Figure 2*.

To ensure the safety of the data used in this study, the input health tweet dataset is encrypted before being stored in the cloud. Ethereum smart contracts are used to store data that is available in the blockchain network and to fulfil the duties of monitoring and tracking data access behaviour using a ciphertext-policy attribute-based security mechanism. An optimised key generation procedure is employed to encrypt the Twitter data series with the help of the upgraded HES and the PF-MLP. To further establish which security method is best for protecting the health tweet dataset, evidence for the techniques' efficacy and protection level is provided. The ISSO method is employed because it provides the best possible answer for creating the secret keys required for deciphering data. In this context, a number of cloud service providers are available. Encrypted data is stored on many cloud services.

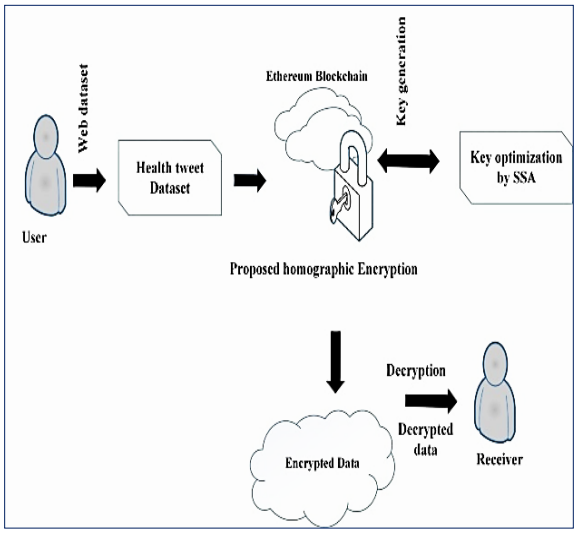

Figure 2 Proposed framework

3.1Ethereum blockchain cloud storage

In this method, smart contracts are used to hold information about password-protected files. Data holders and consumers also use Ethereum smart contracts to store and retrieve ciphertext data for usage in encryption and decryption processes. Each agreement execution is recorded on the distributed ledger. As a consequence, information cannot be altered or denied after it has been transferred between data processors and information owners. The suggested method consists of four parts: the Ethereum blockchain, the data consumer, the data owner, and a cloud server.

A cloud server (host server) is a web-based server that participates in cloud computing. It is produced, stored, and made available online through a cloud computing platform and may be accessed from any location. They are also known as virtual private servers (VPS). The servers in the cloud are completely self-sufficient and include all required applications responsible for storing and maintaining the encrypted user data files.

Ethereum is a blockchain platform where developers can freely build decentralized applications (dApps). It allows the creation of smart contract functionalities using data storage and retrieval interfaces. Owners are responsible for creating and deploying smart contracts, supplying encrypted files, defining security rules, assigning characteristic sets, and granting legitimate access durations to users of their data.

Information consumer regaining access to a password-protected file housed on a remote server. When its characteristic set fits the access architecture contained in a certain ciphertext, it is able to decode the transmitted ciphertext and recover the information key required to unlock the encrypted file.

Here are the stages that represent data storage in the cloud.
Step 1: Data owner has implemented the Storage smart contract on Ethereum.
Step 2: The contract IP is provided once the smart contract has been properly implemented.
Step 3: The data owner holds the smart contract's H(ID), the document ID hash.
Step 4: Data owner submit the encrypted file Eck to the cloud server after packaging the contract address, file ID, and contract Address.
Step 5: The data owner logs the file path received by the cloud service.
Step 6: The secret key to the encoded record's ciphertext is kept by data owner in Ethereum.
Step 7: Data user contacts data owner with an access request.
Step 8: The actual term is added by data owner to data user and stored in the smart contract's database.
Step 9: Data owner saves the secret key of data user in the smart contract after encrypting it.
Step 10: Data owner uses a secure connection to deliver the contract IP and user data.
Step11: Data user retrieves a cloud server's encoded file.
Step 12: Data user determines the smart contract's relevant duration.
Step 13: The smart contract provides data user with the ciphertext for his secret key.

Following this, the HE processes take place, which are mentioned in the section 3.2.

3.2Homomorphic encryption (HE)

Gentry and Halevi [38] were the first to propose a fully homomorphic encryption (FHE) system, and subsequent research has introduced several variations on the core concept. The majority of these computationally intensive security-efficient approaches can only be used so many times before decryption gets unfeasible. This obviously restricts their usefulness in practical situations. Deep learning and data evaluation often face challenges when combined, due to issues such as computations that are many orders of magnitude slower than their plaintext counterparts, accumulated noise that limits the number of operations that can be performed, and the fact that all computations are performed modulo N [39].

Data encryption is one of the critical security measures utilised to ensure the confidentiality of data retained in the cloud. In this paper, an ISSO-based HES process is primarily used to improve the extended protection for cloud information while reducing computational intricacies. Prior to encryption, the ISSO strategy is used to generate keys, which offers the optimal variable for generating keys. The tweet health dataset is then encrypted using the HE requirement, which is a sophisticated security measure widely utilized by numerous real-time implementation processes. The primary objective of using this method in this case is to improve the protection of cloud data by using optimal keys. This sort of encryption is categorised as additive Homomorphic depending on the way it works which is mentioned in Equations 1 and 2:

$$Enyp(x+y) = Enyp(x) \otimes Enyp(y) \quad (1)$$

$$Enyp(\sum u_m) = \prod Enyp\,(u_m) \quad (2)$$

In 1999, Paillier invented the Paillier algorithm, a form of probabilistic public key crypto scheme that utilizes a high order residual class. The following is a definition of the encryption method.

Key generation

Take Set a = u × v and $\lambda = lcm\,(u-1)(v-1)$(3)

In the Equation 3, ‘a’ denotes the set, u and v denotes the large prime number and then randomly selected base $g \in Z_{n^2}^*$, by using the Equation 4.

$$\gcd\left(L\left(g^{\lambda} mod n^2\right)n\right) = 1 \quad (4)$$

Where L is the function and it could be defined as $L(p) = \frac{p-1}{n}$, where (n, g) denotes the public key. Now, the pair (u, v) is still considered to be private whereas (n, g) is viewed as public keys.

Encryption

Considering the selection of a random number of $r \in Z_n$ and the plaintext $m \in Z_n^*$, the ciphertext is defined as shown in Equation 5:

$$c = Eny(m) = g^m r^n mod n^2 \quad (5)$$

In the Equation 5, c indicates the ciphertext, m indicates the plaintext, r denotes the random number.

Decryption

For the ciphertext $c \in Z_{n_2}^*$, Equation 6 shows the value of plaintext m:

$$m = D(c) = \frac{L(c^{\lambda} mod n^2)}{L(g^{\lambda} mod n^2)} mod n \quad (6)$$

It is evident that the additive homomorphism of Paillier's public key encryption technique exists, and the proving procedure is mentioned in Equation 7 and Equation 8:

$$E(m_1) \times E(m_2) = (g^{m_1} r_1^n mod n^2) \times (g^{m_2} r_2^n mod n^2) = g^{m_1+m_2}(r_1 r_2)^n mod n^2 \quad (7)$$

$$E(m_1 + m_2) = g^{m_1+m_2} r^n mod n^2 \quad (8)$$

Where r is the random number. Take r =$r_1 \times r_2$, then E ($m_1 + m_2$) = $E(m_1) \times E(m_2)$ are satisfied.

3.3Key generation based on ISSO

The salp swarm algorithm (SSA) was developed to address a variety of optimisation issues [3]. It imitates the behaviour of salps, a kind of planktonic tunicate that belongs to the Salpidae group and has a barrel-like structure. Moreover, their tissues resemble those of jellyfish, and their substantial water content in weight and movement is another similarity to jellyfish [40]. They move by expanding, and changing their postures requires pumping water throughout their jellied bodies. Salps in seas engage in a swarm behaviour known as the salp chain, which may aid in feeding and improved locomotion via swift harmonious adjustments [41, 42]. Based on this behaviour, a mathematical model was created of the salp chains and tested it using optimisation issues [3].

The primary goal of employing this optimisation technique in this case is to enhance the effectiveness of cryptographic strategies. ISSO is a prevalent and cutting-edge optimization algorithm. It is increasingly being utilized by numerous application frameworks to solve complicated optimisation issues. In particular, it resembles the behavior of salps from the Salpidae family, where the inhabitants are divided into clusters of leaders and subordinates. The salpsis position is established in n-dimensional search spaces, where n represents the problem factors. Salps' status is then altered based on how it searches for food.

The salps' location is found in n-dimensional search spaces, where n represents the factors in the issue. Salps then adjust their location according to their food-finding strategy. The following is the model utilized in order to alter the leader's position. Equation 9 shows the change in position of leader:

$$sp_v^1 = \begin{cases} fsp_v + r_1\left((UB_v - LB_v)r_2 + LB_v\right)r_3 \geq 0 \\ fsp_v - r_1\left((UB_v - LB_v)r_2 + LB_v\right)r_3 < 0 \end{cases} \quad (9)$$

Equation 9, $sp_v^1$is the status of the leader salp in the v^{th} size, UB_v andLB_v denote the upper and lower bound values of the v^{th} dimension, respectively, $r_1, r_2 and r_3$denote the random numbers. This model allows the leader salp to just change its position in relation to the food supply. The quantity r_1 is then regarded as the most crucial ISSO parameter since it aids in striking a balance between the capabilities of exploring and exploiting, presented in Equation 10:

$$r_1 = 2e^{-\left(\frac{4p}{M}\right)^2} \quad (10)$$

Where p stands for the currently occurring iteration and M for the maximum number of iterations. As a result, the parameters $r_2 and\ r_3$ are random number where [0, 1] and [0, 1] represent the obtained random values. The accompanying numerical simulations is then used to modify the positions of followers (Equation 11):

$$sp_v^1 = \frac{1}{2} g t^2 + f_0(t) \quad (11)$$

In Equation 11, time is denoted as t, initial speed is denoted as f_0 and the value of g is computed using the Equation 12:

$$g = \frac{f_{final}}{f_0} and f = \frac{s - s_0}{t} \quad (12)$$

As a result, the position of the followers is likewise changed using the Equation 13:

$$sp_v^1 = \frac{1}{2}(sp_v^1 + sp_v^{u-1}) \quad (13)$$

Where $u \geq 2$ and sp_v^1stand for the follower's location in the v^{th} dimension. The best ideal solution, which aids in choosing the variables utilised to generate the keys, is found using this process, and its operational flow is represented in *Figure 3*.

3.3.1 PF-MLP based encryption

A PF-MLP-based encryption framework is additionally employed in this work to enhance data protection before storing it in the cloud systems. The primary benefit of employing this method is that it effectively protects the information from unauthorized third-party access. It also shields original data information effectively with fewer computational processes. Even if attackers gain the server's credentials, they will be unable to access the original data. Since it's more challenging for hackers to recognise encrypted information, they are unable to gather information as quickly. For the encryption and decryption of data, the PF-MLP method typically requires a key pair created with best ISSO solution.

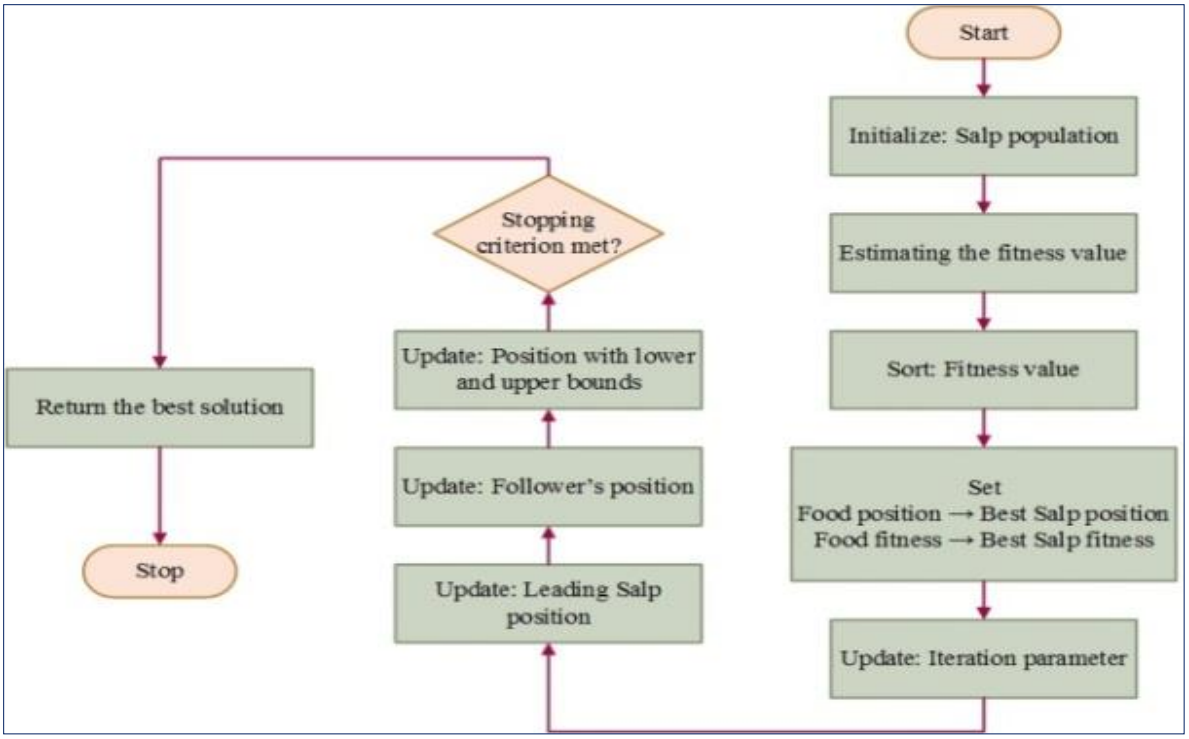

Figure 3 ISSO flow diagram

Algorithm: Paillier Federated Multi-Layer Perceptron Encryption

Input: Health tweet dataset
Output: Model variable β_x;
Stage 1: Based on the optimal solution of ISSO key pair is generated.
Stage 2: Initialize model parameter;
Stage 3: For 'u' in iteration do
Stage 4: Apply forward propagation

$$M_u = Forwardpropagation\ (\beta_u, \beta_u)$$

Stage 5: Loss function estimation:
Loss$L_u = Loss(F^*(\beta_u), \beta_u)$: $If\ L_u < \varepsilon then$
Break;
Else
Apply back propagation as follows:
$N_u = Backpropagation(\beta_u, \beta_u, L_u)$;
Public key is used to encrypt data, as illustrated below:
Encryption (N_u) =$Enyp_{paillier}(Pu_{key}, L_u)$;
Encrypted data is shared to the cloud server in the form of $Enyp(N_u)$;
It is received by the server in the form of $Enyp(L_{unew})$;
In the following way the private key is employed to decrypt the data at the receiving end:

$$N_u = DeC_{pallier}(Pvt_{key}, Enyp(N_u))$$

Update $\beta_{u+1} = \beta_u - lr \times D_{new}$;
End if;
End for;
Stage 6: Provide the model parameter back asβ_f;

4.Results and discussion

The system was implemented using Python software frameworks, which are known for their versatility and extensive library support. The outcomes of the proposed ISSO-based PF-MLP process were verified and tested using a variety of assessment indicators. The results demonstrate the superiority of the suggested strategy by comparing it with more contemporary encryption methods based on optimization.

The dataset includes 732 records categorized under user and platforms, featuring attributes such as text, sentiments, timestamps, user details, platform, hashtags, retweets, likes, and geographical and temporal data like country, year, month, day, and hour. The focused parameters are retweets, likes, and year, and the data is sourced from the Kaggle repository. The tweet health dataset is utilized as processing input to evaluate the efficiency of the system.

The evaluation employed various types of measurements such as encryption and decryption times, processing time, upload and download speeds, and the total number of packets delivered.

Figure 4 presents an ISSO-based optimization approach used to evaluate the HES encryption time. According to the results, the proposed approach processed 10 MB of data in 800 ms. In comparison, processing 10 MB of data using conventional elliptic curve cryptography (ECC) [43] and RSA [44] techniques took 1100 ms and 1500 ms, respectively.

The decryption time of the proposed method for 10 MB of data using HES with ISSO-based optimization was 900 ms, as shown in *Figure 5*. Comparable results were obtained with 10 MB of data using traditional methods such as ECC and RSA, which took 1100 ms and 1500 ms, respectively. These findings indicate that the ISSO-based PF-MLP technique requires less time for decryption compared to the other strategies. The processing of the proposed ISSO-based PF-MLP approach, along with existing ECC and RSA methods, is validated and compared in *Figure 6*. According to the results, the proposed methodology processed 10 MB of data in 1500 ms. The same 10 MB of data was encrypted using conventional ECC and RSA techniques at 1600 ms and 1900 ms, respectively. These comparative analyses lead to the conclusion that the suggested ISSO-based PF-MLP technique offers reduced encryption, decryption, and processing times compared to the other methods. *Figure 7* validates the total number of correctly received packets for the proposed ISSO-based PF-MLP approach, as well as for the current ECC and RSA methods. The findings demonstrate that the ISSO-based PF-MLP combination successfully received 98% of the packets. In comparison, RSA and ECC achieved success rates of 89% and 82%, respectively. *Figure 8* shows the uploading and downloading times. This clearly demonstrates that the ISSO-based PF-MLP delivers the best outcomes in terms of received packets compared to other strategies. The results demonstrate that for 10 MB of data, the ISSO-based PF-MLP requires 4 ms, whereas ECC [43] and RSA [44] require 7 ms and 9 ms, respectively. *Figure 9* presents the downloading time analysis, showing that the ISSO-based PF-MLP achieved 6 ms for 10 MB of data. Similarly, the ECC and RSA methods required 9 ms and 12 ms, respectively.

Table 1 presents a comparison of the performance metrics between the prior RSA-based research and the proposed model. The proposed model demonstrates significant improvements across multiple metrics. Specifically, the throughput increased from 100 Mbps to 120 Mbps, showcasing a 20% improvement. Latency, measured in milliseconds, decreased from 50 ms to 30 ms, indicating a 40% reduction. Resource utilization, expressed as a percentage, improved from 75% to 60%, reflecting a 20% enhancement. Additionally, energy efficiency, measured in Joules per Megabit (J/Mb), improved from 10 to 12, representing a 20% boost. These results underscore the superior performance of the proposed model in terms of throughput, latency, resource utilization, and energy efficiency compared to the prior RSA-based research.

The enhanced performance of the proposed approach in securely storing data on the Ethereum blockchain is demonstrated in *Table 2*. With a low error rate of 0.13%, it outperforms both ECC [43] and RSA [44], offering a more reliable and accurate method for cryptographic operations. This highlights its potential for improved data security and integrity.

A complete list of abbreviations is listed in *Appendix I.*

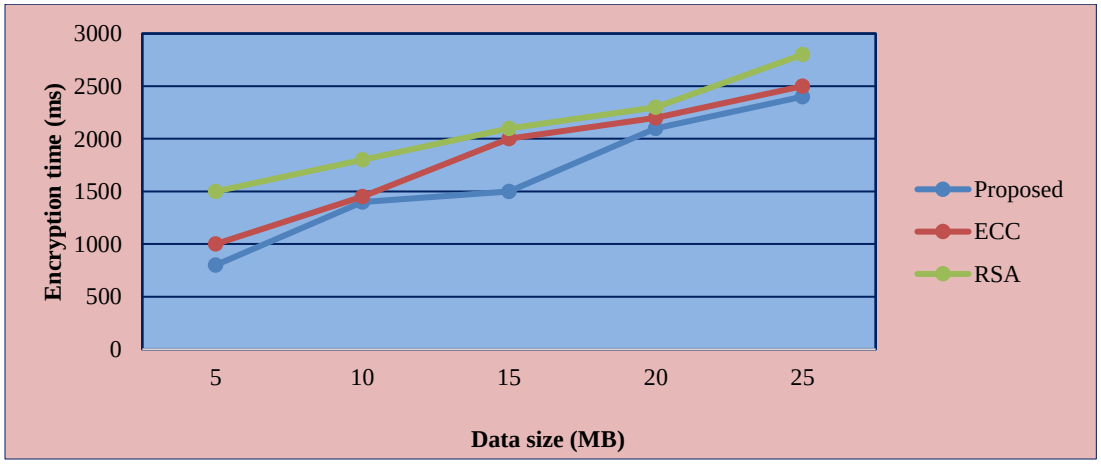

Figure 4 Encryption time comparison with different data size

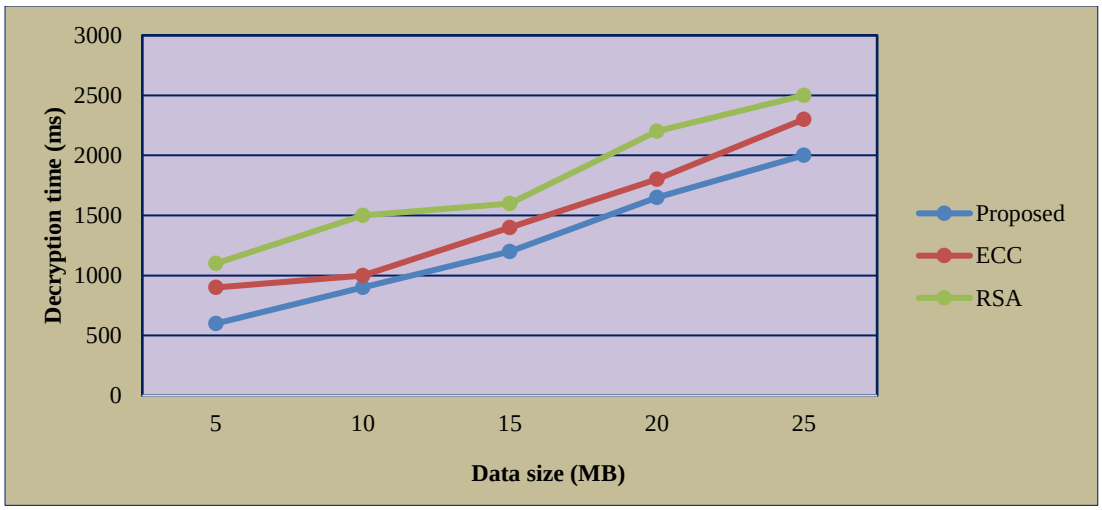

Figure 5 Decryption time comparison with different data size

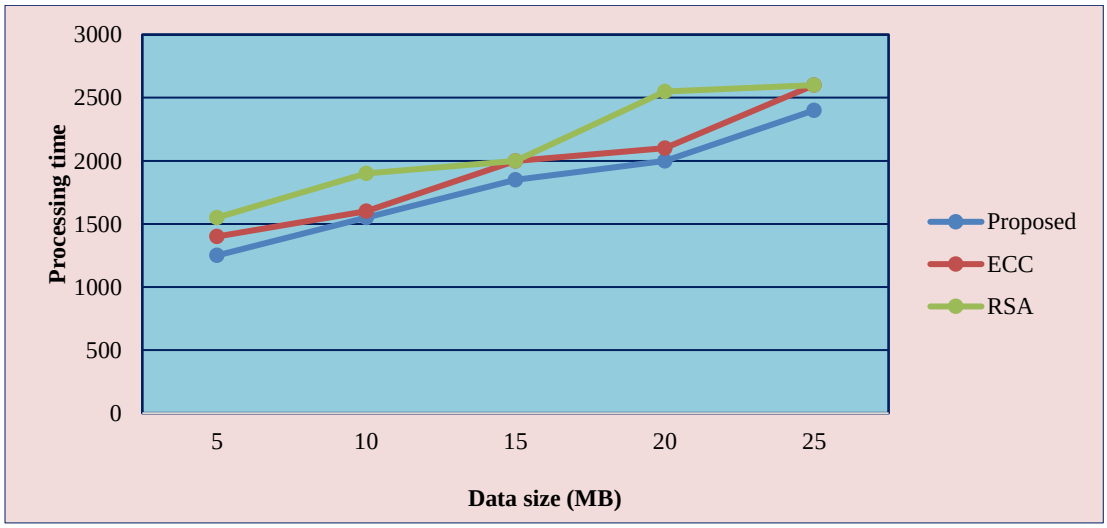

Figure 6 Processing time comparison with different data size

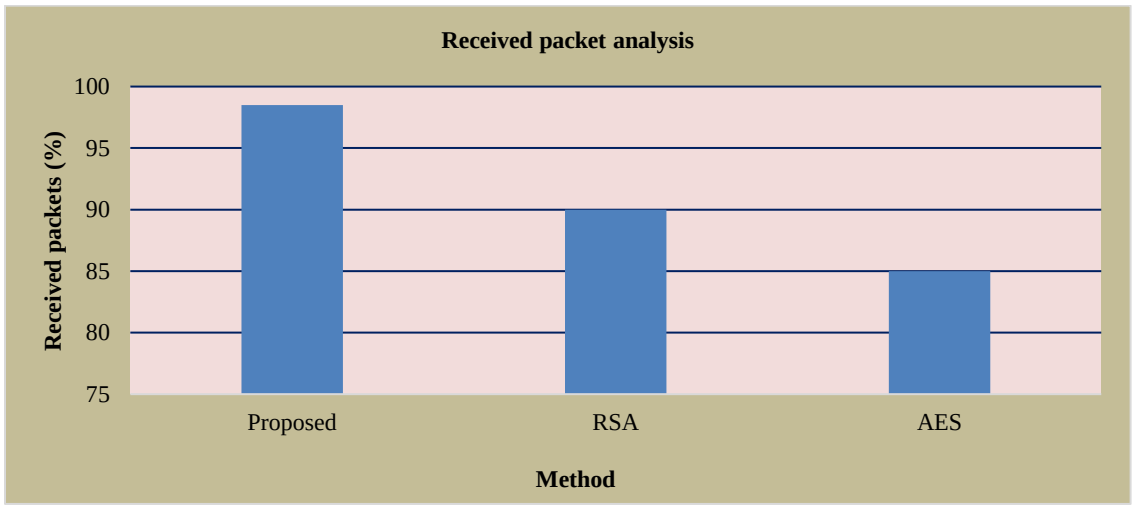

Figure 7 Received packet analysis comparison

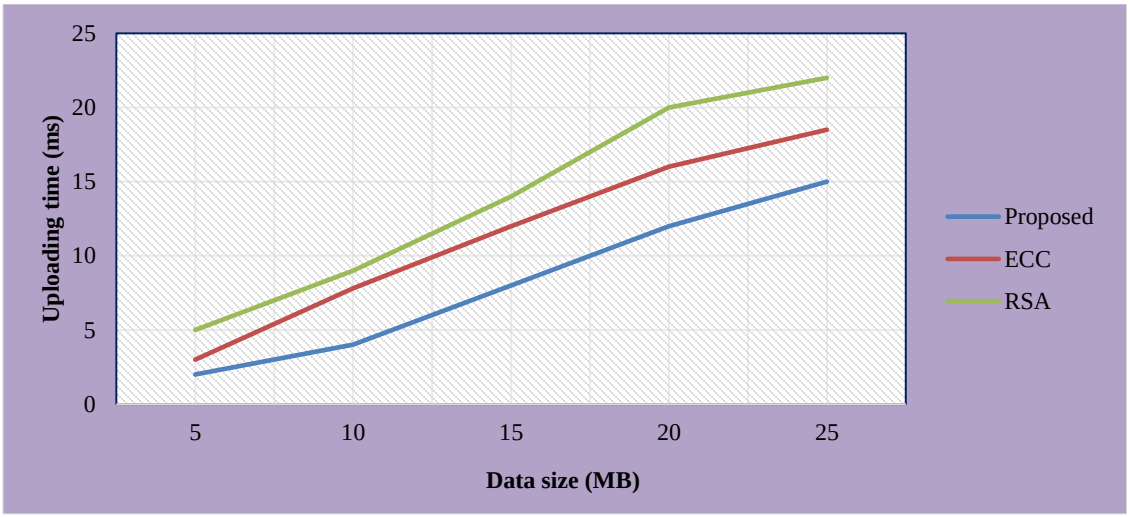

Figure 8 Uploading time comparison with different data size

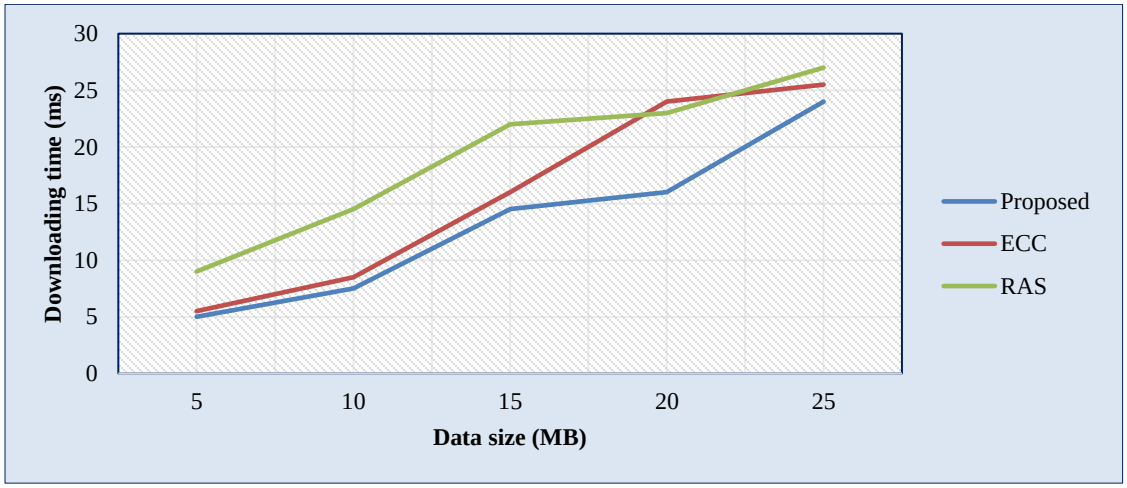

Figure 9 Downloading time comparison with different data size

Table 1 Comparison of RSA and the proposed approach considering different performance measures

Metric	RSA	Proposed approach
Throughput (Mbps)	100	120
Latency (ms)	50	30
Resource utilization (%)	75	60
Energy Efficiency (J/Mb)	10	12

Table 2 Error rate comparison

Method	Error rate
ECC	0.6%
RSA	0.35%
Proposed	0.13%

5.Conclusion and future work

The research presents a hybrid ISSO-based PF-MLP mechanism aimed at enhancing data privacy and security. The key contribution of this work lies in the application of optimization-based cryptographic approaches to bolster the security of the health tweet dataset. The ISSO technique is particularly notable for its ability to generate parameters essential for secret key construction, which is crucial for both data encryption and decryption. The proposed ISSO-based PF-MLP approach offers several significant advantages, including optimal performance, reduced processing time, and increased operational speed. These improvements make it a highly efficient solution for securing sensitive data. The performance and efficacy of the ISSO-based PF-MLP technique have been rigorously analyzed, validated, and compared using various performance metrics. The evaluations clearly demonstrate that the combination of ISSO and PF-MLP outperforms alternative strategies, establishing it as a superior method for enhancing data privacy and secrecy. The future work

will focus on emphasizing the safeguarding of data, privacy, and digital communication. One of the key challenges facing encryption is the advent of quantum computers, which have the potential to break many existing encryption algorithms. To counter this threat, quantum-resistant encryption methods will be developed in the future work.

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

Data availability
The dataset used for the experiments is publicly available at https://www.kaggle.com/datasets/kashishparmar02/social-media-sentiments-analysis-dataset.

Author's contribution statement
R.S.Kanakasabapathi: Conceptualization, investigation, data collection, writing – review and editing. **J.E.Judith**: Supervision, writing – review and editing.

References
[1] Groom FM, Jones SS. Enterprise cloud computing for non-engineers. CRC Press; 2018.
[2] Thabit F, Alhomdy SA, Alahdal A, Jagtap SB. Exploration of security challenges in cloud computing: issues, threats, and attacks with their alleviating techniques. Journal of Information and Computational Science. 2020; 12(10).
[3] Mirjalili S, Gandomi AH, Mirjalili SZ, Saremi S, Faris H, Mirjalili SM. Salp swarm algorithm: a bio-inspired optimizer for engineering design problems. Advances in Engineering Software. 2017; 114:163-91.
[4] C. Thomas, Data Mining. BoD-Books on Demand; 2018.
[5] Rachmat N, Samsuryadi. Performance analysis of 256-bit AES encryption algorithm on android smartphone. In journal of physics: conference series 2019 (pp. 1-6). IOP Publishing.
[6] Du W, Deng J, Han YS, Varshney PK, Katz J, Khalili A. A pairwise key predistribution scheme for wireless sensor networks. ACM Transactions on Information and System Security. 2005; 8(2):228-58.
[7] Singh S, Jeong YS, Park JH. A survey on cloud computing security: issues, threats, and solutions. Journal of Network and Computer Applications. 2016; 75:200-22.
[8] Sagar RG, Kumar NA. Encryption based framework for cloud databases using AES algorithm. International Journal of Research Studies in Computer Science and Engineering. 2015.
[9] Goodfellow I. Deep learning. MIT Press; 2016.
[10] Gu J, Wang Z, Kuen J, Ma L, Shahroudy A, Shuai B, et al. Recent advances in convolutional neural networks. Pattern Recognition. 2018; 77:354-77.
[11] Rivest RL, Adleman L, Dertouzos ML. On data banks and privacy homomorphisms. Foundations of Secure Computation. 1978; 4(11):169-80.
[12] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978; 21(2):120-6.
[13] Migliore V, Bonnoron G, Fontaine C. Practical parameters for somewhat homomorphic encryption schemes on binary circuits. IEEE Transactions on Computers. 2018; 67(11):1550-60.
[14] Mojisola FO, Misra S, Febisola CF, Abayomi-alli O, Sengul G. An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA). Egyptian Informatics Journal. 2022; 23(2):291-301.
[15] Shinde MR, Taur RD. Encryption algorithm for data security and privacy in cloud storage. American Journal of Computer Science and Engineering Survey. 2015; 3(1):34-9.
[16] Sangeetha SK, Vanithadevi V, Rathika SK. Enhancing cloud security through efficient fragment based encryption. International Journal of Pure and Applied Mathematics. 2018; 118(18):2425-36.
[17] Arockiam L, Monikandan S. Data security and privacy in cloud storage using hybrid symmetric encryption algorithm. International Journal of Advanced Research in Computer and Communication Engineering. 2013; 2(8):3064-70.
[18] Wang C, Ren K, Wang J. Secure optimization computation outsourcing in cloud computing: a case study of linear programming. IEEE Transactions on Computers. 2015; 65(1):216-29.
[19] George GM, Jayashree LS. Ethereum blockchain-based authentication approach for data sharing in cloud storage model. Cybernetics and Systems. 2023; 54(6):961-84.
[20] Sheeba TB, Hemanth SV, Devaraj V, Arularasan AN, Gopianand M. Digital hash data encryption for iot financial transactions using blockchain security in the cloud. International Journal on Recent and Innovation Trends in Computing and Communication. 2023; 11:129-34.
[21] Panda SK, Mishra V, Dash SP, Pani AK. Recent advances in blockchain technology: real-world applications. Springer Nature; 2023.
[22] Dule CS, Roopashree HR. Privacy preservation modelling for securing image data using novel ethereum-based ecosystem. International Journal of Advanced Computer Science and Applications. 2023;14(2):126-35.
[23] Antony SM, Samiappan D. IPFS based file storage access control and authentication model for secure data transfer using block chain technique. Concurrency and Computation: Practice and Experience. 2023; 35(2):e7485.
[24] Sucharitha G, Sitharamulu V, Mohanty SN, Matta A, Jose D. Enhancing secure communication in the cloud through blockchain assisted-CP-DABE. IEEE Access. 2023; 11: 99005-15.

[25] Mahajan H, Reddy KT. Secure gene profile data processing using lightweight cryptography and blockchain. Cluster Computing. 2024; 27(3):2785-803.
[26] Almasian M, Shafieinejad A. Secure cloud file sharing scheme using blockchain and attribute-based encryption. Computer Standards & Interfaces. 2024; 87:103745.
[27] Kallapu B, Dodmane R, Thota S, Sahu AK. Enhancing cloud communication security: a blockchain-powered framework with attribute-aware encryption. Electronics. 2023; 12(18):1-15.
[28] Verma G, Kanrar S. Secure document sharing model based on blockchain technology and attribute-based encryption. Multimedia Tools and Applications. 2024; 83(6):16377-94.
[29] Sajay KR, Babu SS, Vijayalakshmi Y. Enhancing the security of cloud data using hybrid encryption algorithm. Journal of Ambient Intelligence and Humanized Computing. 2019:1-10.
[30] Zhao F, Li C, Liu CF. A cloud computing security solution based on fully homomorphic encryption. In 16th international conference on advanced communication technology 2014 (pp. 485-8). IEEE.
[31] Das D. Secure cloud computing algorithm using homomorphic encryption and multi-party computation. In international conference on information networking 2018 (pp. 391-6). IEEE.
[32] Joseph M, Mohan G. Design a hybrid optimization and homomorphic encryption for securing data in a cloud environment. International Journal of Computer Networks and Applications. 2022; 9(4):387-95.
[33] Kumar KS, Nair SA, Roy DG, Rajalingam B, Kumar RS. Security and privacy-aware artificial intrusion detection system using federated machine learning. Computers & Electrical Engineering. 2021; 96:107440.
[34] Dumbere DM, Ambhaikar A. An ML bio-inspired model for improving security and speed of FHE for cybersecurity. In IEEE international conference on technology, research, and innovation for betterment of society 2021 (pp. 1-8). IEEE.
[35] Soykan EU, Karacay L, Karakoc F, Tomur E. A survey and guideline on privacy enhancing technologies for collaborative machine learning. IEEE Access. 2022; 10:97495-519.
[36] Loftus TJ, Ruppert MM, Shickel B, Ozrazgat-Baslanti T, Balch JA, Efron PA, et al. Federated learning for preserving data privacy in collaborative healthcare research. Digital Health. 2022: 20552076221134455.
[37] Harasic M, Keese FS, Mattern D, Paschke A. Recent advances and future challenges in federated recommender systems. International Journal of Data Science and Analytics. 2024; 17(4):337-57.
[38] Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. In annual international conference on the theory and applications of cryptographic techniques 2011 (pp. 129-48). Berlin, Heidelberg: Springer Berlin Heidelberg.
[39] Ahmed EY, Elkettani MD. Fully homomorphic encryption: state of art and comparison. International Journal of Computer Science and Information Security. 2016; 14(4):159-67.
[40] Henschke N, Everett JD, Richardson AJ, Suthers IM. Rethinking the role of salps in the ocean. Trends in Ecology & Evolution. 2016; 31(9):720-33.
[41] Anderson PA, Bone Q. Communication between individuals in salp chains. II. physiology. Proceedings of the Royal Society of London. Series B. Biological Sciences. 1980; 210(1181):559-74.
[42] Sutherland KR, Weihs D. Hydrodynamic advantages of swimming by salp chains. Journal of The Royal Society Interface. 2017; 14(133):20170298.
[43] Christo MS, Jesi VE, Priyadarsini U, Anbarasu V, Venugopal H, Karuppiah M. Ensuring improved security in medical data using ECC and blockchain technology with edge devices. Security and Communication Networks. 2021; 2021(1):6966206.
[44] Ge C, Liu Z, Fang L. A blockchain based decentralized data security mechanism for the internet of things. Journal of Parallel and Distributed Computing. 2020; 141:1-9.

R.S.Kanakasabapathi is currently pursuing his Ph.D. in Computer Applications at Noorul Islam Centre for Higher Education, Kumarakoil. He obtained his MCA degree from James College of Engineering and Technology, Navalkadu, and his B.Sc. degree in Computer Science from S.T. Hindu College, Nagercoil. His research interests include Cloud Computing, Data Mining, and Image Processing.
Email: sabapathiravanan93@gmail.com

Dr. J.E.Judith is a Professor in Computer Science and Engineering at Noorul Islam Centre for Higher Education, Kumaracoil. She earned her Bachelor's degree in Computer Science and Engineering from Noorul Islam College of Engineering in 2003, followed by a Master's degree in Computer Science and Engineering from Karunya University in 2006. She completed her Ph.D. in Computer Science and Engineering at Noorul Islam Centre for Higher Education in 2015. Dr. Judith has over 18 years of teaching and research experience and has published numerous research papers in national and international journals. Her research interests include Data Mining, Big Data Analytics, Hadoop and Distributed Systems, and Machine Learning Techniques.
Email: judith@niuniv.com

Appendix I

S. No.	Abbreviation	Description
1	ABE	Attribute-Based Encryption
2	ACO	Ant Colony Optimisation
3	AES	Advanced Encryption Standard
4	BA-CP-DABE	Blockchain-Assisted Ciphertext Policy Decentralized Attribute-Based Encryption
5	BCO	Bee Colony Optimisation
6	CP-ABE	Ciphertext-Policy Attribute-Based Encryption
7	CSA	Cloud Security Alliance
8	dApps	Decentralized Applications
9	D-GET	Decentralized Gateway for Energy Transactions
10	DHDE	Digital Hash Data Encryption
11	ECC	Elliptic Curve Cryptography
12	EHR	Electronic Health Record
13	FA	Firefly Algorithm
14	FL	Federated Learning
15	FHE	Fully Homomorphic Encryption
16	HE	Homomorphic Encryption
17	HES	Homomorphic Encryption Standard
18	IoT	Internet of Things
19	IPFS	Interplanetary File System
20	ISO	International Organization for Standardization
21	ISSO	Improved Salp Swarm Optimization
22	J/Mb	Joules Per Megabit
23	LP	Linear Programming
24	MD5	Message Digest 5
25	Ms	Millisecond
26	OAEP	Optimal Asymmetric Encryption Padding
27	PF-MLP	Paillier Federated Multi-Layer Perceptron
28	PSO	Particle Swarm Optimisation
29	RSA	Rivest–Shamir–Adleman algorithm
30	SSA	Salp Swarm Algorithm
31	SWHE	Sweeping Homomorphic Encryption
32	TTP	Trusted Third Parties
33	VPS	Virtual Private Servers
34	WO	Whale Optimisation