A Novel Privacy-Preserving Approach Using Optimized Deep Learning for Secure Data Mining

Rahul Reddy Bandhela
CVS Pharmacy Inc., Sudbury, MA, USA
Rahulreddy9725@gmail.com (corresponding author)

RamMohan Reddy Kundavaram
Dynamic Technology Inc., Naperville, IL, USA
Rkundavaram_GPS@nec.edu

Abhishake Reddy Onteddu
DPR Solutions Inc., Aurora, IL, USA
Ontedduabhishakereddy@gmail.com

Received: 22 October 2025 | Revised: 26 November 2025, 26 December 2025, 3 January 2026, and 6 January 2026 | Accepted: 9 January 2026

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | *DOI: https://doi.org/10.48084/etasr.15710*

ABSTRACT

Preservation of privacy involves the use of methods to protect sensitive data. Data mining is the derivation of various patterns and insights from big data using statistical and machine learning tools. A privacy-preserving data mining protocol follows a methodological system to ensure the safety of data encryption, improving key generation. The proposed system architecture offers a strong cloud-based platform for data encryption and retrieval. Data preservation is performed using Brakerski/Fan-Vercauteren (BFV), where data is encrypted with the help of a secret key and transformed with the help of a random matrix to increase security. The secret key is constructed using the Double Exponential Smoothing Secretary Bird Optimization Algorithm (DES-SBOA), combining the double exponential smoothing with the Secretary Bird Optimization Algorithm (SBOA). The encrypted data is stored safely in the cloud, ensuring that it will not be accessed by the wrong users, but can still be used to produce MLP outputs with an accuracy of 57.5%, a privacy of 39.8%, a utility of 98.5%, a fitness of 62.9%, and an execution time of 341.5s.

Keywords-BFV homomorphic encryption; Double Exponential Smoothing Secretary Bird Optimization Algorithm (DES-SBOA); MLP; privacy preservation

I. INTRODUCTION

Cloud computing refers to the storage, processing, and management of data using internet-based servers, eliminating the need for expensive local infrastructure. Although scalable and cost-effective, cloud computing increases the risks of privacy and security, including breach, unauthorized access, and misuse [1]. Some mitigation mechanisms involve encryption, access control, anonymization, and homomorphic encryption, which allow computations to be run on encrypted data [2]. Due to the booming expansion of the cloud, IoT, and big data, privacy has become a major concern [3]. Federated learning, homomorphic encryption, and Secure Multi-Party Computation (SMPC) are some of the techniques that enable data processing on encrypted data without decrypting it.

In [1], a privacy-preservation mechanism for IIoT involved two stages, i.e., data restoration and sanitization. Sanitization conceals important information to avoid unauthorized leakage, and an ideal encryption key is produced using the G-BHO method. Key generation was guided by a multi-objective function based on alteration rate, hiding ratio, and correlation, and experiments verified high security and privacy compared to current methods. In [4], GANs were compared with differential privacy to improve data protection in IIoT. This approach, tested in both public and industrial datasets, protected sensitive data while ensuring model stability, as indicated by the R^2 results.

In [5], a blockchain architecture, based on Ethereum, used the ABC-ROA hybrid optimization algorithm for key generation during data transmission, achieving balanced multi-objective formulations for IP rate, DM, FR generation, and HF rate, resulting in increased security in blockchain-based sharing. In [6], the focus was on secure outsourcing of spectral clustering in a multi-user cloud environment. This study constructed a scalable spectral clustering scheme using BFV homomorphic encryption and a two-server non-collusive

model, which provided accuracy and guaranteed privacy protection. PCM2 [7] is a privacy-oriented multimedia mobile cloud computing framework that addresses bandwidth and resource limitations. A perturbation-based compression method minimized bandwidth consumption and latency and optimized power efficiency, which is very effective for cloud-based mobile applications. In [8], homomorphic encryption and blockchain were used to protect privacy in IoT healthcare applications. Data encryption ensured patient privacy, and smart contracts, based on blockchain, ensured fine-grained access control and audit trails. This approach achieved fewer communication expenses and greater transparency. AFBS_WOA [9] is a hybrid key-generation method for cloud-based healthcare data. Using AFBS and WOA, this approach creates key matrices that guarantee privacy-preserved databases, and access to them is possible through secret key sharing.

A. *Challenges*

Despite advances, there are still some research gaps:

- Scalability: ABC-ROA [10] offers high-security in blockchain-based information sharing, but needs to be extended to accomplish decentralized and real-time monitoring of the global supply chain.
- Dynamic publishing: HAEF [11] builds on anonymization and data accessibility but not on dynamic, massive, and real-time publishing with privacy preservation in a distributed setup.
- Higher stage optimization: AFBS_WOA [12] improved privacy-utility trade-offs but was not tested using more up-to-date optimization algorithms or diverse datasets to enhance adaptability and performance.

This study introduces a privacy-preserving data mining system based on BFV homomorphic encryption, supplemented with randomized matrix transformation and an improved generation of the secret key using the Double Exponential Smoothing Secretary Bird Optimization Algorithm (DES-SBOA). SHA-256 is used to authenticate users for secure decryption. The major contributions are: (i) time-optimized key generation by developing DES-SBOA, (ii) key retrieval using a 256-bit hash algorithm for authentication, and (iii) analysis of accuracy, privacy, utility, convergence, fitness, and execution time.

II. SYSTEM MODEL

The system model in Figure 1 represents a secure framework for preserving data privacy utilizing homomorphic encryption and an optimized secret key generation technique. Initially, cloud data is encrypted before storage using homomorphic encryption, ensuring that computations can be performed on encrypted data. DES-SBOA is used to generate a secure secret key, which enhances the robustness of encryption. The encrypted data is then stored in the cloud. When data restoration is required, a key-based authentication mechanism allows access only if the correct key is provided. Upon successful authentication, the encrypted data is decrypted and restored to its original form. This framework ensures confidentiality, integrity, and security throughout the data lifecycle, making it highly suitable for privacy-sensitive settings, such as healthcare systems and the IIoT, where secure data sharing and computation are essential.

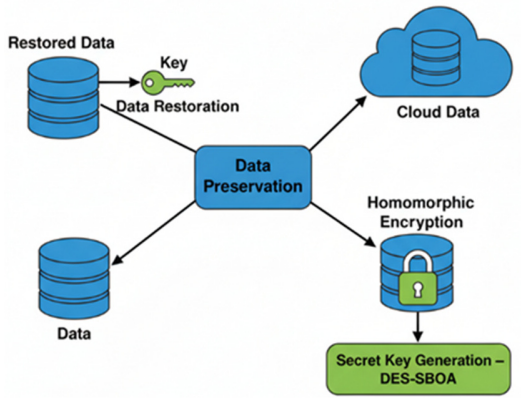


Fig. 1. System model.

III. PROPOSED DES-SBOA BASED MLP METHOD FOR PRIVACY PRESERVATION

This study introduces a data security system that combines the BFV homomorphic encryption and an optimization of the secret key generation. Using BFV to encrypt raw data allows the computation of values without decryption. DES-SBOA produces the secret key, giving it greater encryption strength. The user gives a hash of the secret key during the process of restoration to authenticate him/her; After verification, the encrypted data is then retrieved and decrypted. Figure 2 depicts the architecture.

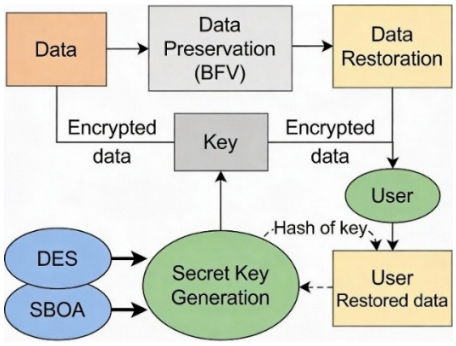


Fig. 2. Architectural illustration of the proposed mechanism.

A. *Optimized Multi-Objective Framework for Privacy Preservation*

The proposed framework integrates BFV homomorphic encryption with DES-SBOA-based key optimization to achieve privacy-preserving data security. BFV enables secure arithmetic on encrypted data without decryption, while DES-SBOA optimizes secret keys for strong encryption and efficient performance. Data integrity is reinforced through Hadamard and Tracy-Singh products, and authentication is enforced through secure hashing. Data is encrypted with a secret key and further protected using an XOR operator with a random kernel

matrix, computed from marginal mean vectors of original and transformed data. Modular arithmetic ensures controlled randomness, while the Tracy-Singh product introduces additional complexity [13].

The combination of BFV homomorphic encryption and secret key optimization based on DES-SBOA ensures strong privacy and efficient computation. Homomorphic encryption allows secure arithmetic operations but not decryption, minimizing the exposure to threats. Security and performance are balanced, and Hadamard and Tracy-Singh products are used to improve integrity and consistency. Strong authentication helps to avoid unauthorized access.

A sumb-based scalar provides controlled randomness, and the Tracy-Singh product further varies. Collectively, these mechanisms provide privacy, integrity, and practicability of the encrypted information, making the framework efficient in privacy-sensitive applications [14].

$$A^*_{p\times q} = B\left(A_{p\times q}, C\right) \oplus r_{1\times q} \quad (1)$$

where A^* is preserved data, A specifies original data with dimensions of $p \times q$, and $B(A, C)$ signifies the encryption of A, using the BFV encryption scheme, with the secret key C, which is generated by DES-SBOA. Each row of the encrypted data is XOR-ed with a random kernel matrix r of size $1 \times q$. This process generates a random transformation matrix to enhance the security of the encryption. Equation (2) represents a modulus operation, where D is divided by E, and the remainder is assigned to $r_{1\times q}$. This operation is widely used in number theory, cryptography, and computer science for hashing and modular arithmetic in encryption algorithms.

$$r_{1\times q} = D \bmod E \quad (2)$$

where D is the transformation matrix derived from the original data, and E is the scaling factor. Equation (3) represents the Hadamard product, which ensures that data properties remain hidden while still being mathematically useful.

$$D_{1\times q} = F \otimes G \quad (3)$$

Here, F is the column-wise mean of the original data, and G is the column-wise mean of the transformed data T. Equations (4) and (5) represent the marginal mean of the data, which aids in preserving its statistical properties.

$$F_{1\times m} = \frac{1}{p}\sum_{i=1}^{p} A_{ij} \quad (4)$$

$$G_{1\times q} = \frac{1}{p}\sum_{i=1}^{p} T_{ij} \quad (5)$$

where A_{ij} denotes the original data values, T_{ij} denotes the transformed data values, and p is the number of elements.

$$E_{1\times 1} = \sum_{i=1}^{P}\sum_{j=1}^{q} T_{ij}\ , \text{ where } P = p \times q \quad (6)$$

$$T_{P\times q} = A_{p\times q} \odot r_{q\times q} \quad (7)$$

B. Secret Key Generation Using DES-SBOA

Secret keys ensure confidentiality, integrity, and resistance against unauthorized access in privacy-preserving systems. In this framework, this process is optimized using DES-SBOA, which combines Double Exponential Smoothing (DES) with the Secretary Bird Optimization Algorithm (SBOA) [15]. DES minimizes fluctuations and maintains trends to use a safe analytics method, and SBOA optimizes key selection with fast convergence, improving the exploration-exploitation trade-off and randomness. Their combination yields safe, non-predictable, and effective keys, and hence, DES-SBOA is very appropriate in cloud-based privacy-preserving encryption.

Secret keys are encoded in forms of numeric vectors optimized using DES-SBOA. Every dimension of the vectors is a cryptographic parameter, which allows for manipulating the variables at the same time and achieving better results. A candidate is a possible solution, as shown in Figure 3. This design enables DES-SBOA to narrow down candidates by iteratively removing those that are weak in terms of security and efficiency.

Fig. 3. Solution encoding.

DES-SBOA incorporates DES into the SBOA [16], increasing its stability and convergence. DES dynamically balances the exploration and exploitation tradeoff by dynamically varying the step sizes, avoiding a priori convergence and local optima [17]. The behavior of secretary birds that inspires SBOA (searching, evaluating, and attacking prey) is a good model for improving the trade-offs in exploration and exploitation, effectively simulating the processes. SBOA, known to be fast converging and adaptable, is effective in complex multivariate spaces. In this method, birds are the candidate solutions, which are randomly placed in the search space as per:

$$Y = L_b + s * (U_b - L_b) \quad (8)$$

where Y denotes the location of the secretary bird, L_b and U_b are the lower and upper bounds, and s is a random number between 0 and 1. SBOA follows a population-based approach, initiating optimization with a set of candidate solutions.

In the search stage, the birds find camouflaged prey by systematic scanning, which is equivalent to searching the solution space. The algorithm analyzes the candidate solutions, narrows down the knowledge of the landscape, and finds the promising areas to be exploited further. This search stage is mathematically expressed as:

$$while\ T < \frac{1}{3}t,\ Y^{T+1} = Y^T + (Y_{s1} - Y_{s2}) * S_1 \quad (9)$$

where Y^{T+1} is the updated position of a secretary bird, Y^T is the position of the best solution found so far, T is the current iteration, N is the total number of secretary birds, t is the total number of iterations, and S_1 is the current position of the bird.

DES is incorporated to enhance the performance of SBOA. Starting from (10), the update rules are progressively refined through substitution and simplification in (11-15). These transformations balance exploration and exploitation by

dynamically adjusting step sizes, preventing premature convergence, and improving adaptability [18]. The final update rule for the secretary bird's position is obtained as:

$$Y^{T+1} = \left(\frac{\omega*(1+\xi)}{\omega*(1+\xi)-1}\right)* \begin{Bmatrix} \left(\frac{\xi*(\omega*Y^{T-1}+(1-\omega)*k^{T-1})-(1-\omega)*k^{T}*(1+\xi)-(1-\xi)*K^{T-1}}{\omega*(1+\xi)}\right) \\ +(Y_{s1}-Y_{s2})*S_1 \end{Bmatrix} \quad (10)$$

where Y_{S1} and Y_{S2} represent random candidate solutions, S_1 is a random array in dimension $1 \times dim$, Y^T is the current solution (secret key candidate), and k^T denotes the secretary bird's strategic movement. In exploitation, SBOA refines the best candidate solutions to converge toward the global optimum. Attacking the prey acts as a decisive refinement, intensifying exploitation by strengthening high-quality solutions and eliminating weaker ones. Next, SBOA employs avoidance strategies to escape local optima and protect solutions from premature convergence. These steps are continuously carried out until the optimal solution is found. Algorithm 1 outlines the proposed DES-SBOA.

```
Algorithm 1: DES-SBOA
Initialize population randomly (t is the
current count of iterations, N is the total
count of secretary birds, and T is the total
count of iterations)
while t=1:T
  Generate a new population
  For i=1:N
    //Exploration (hunting behavior)
    Select a candidate for further evaluation
    Calculate new status of secretary bird
    Evaluate fitness
    //Exploitation (escape strategy)
    Select best candidates from the remaining
    individuals
    Compare each individual's fitness with the
    best found during the exploration phase
  End for
  Save the best solution found so far
End while
Return the best-found solution.
```

C. Optimal Fitness Value Evaluation

DES-SBOA selects the optimal secret key using a multi-objective fitness function that balances privacy, utility, hiding ratio, information preservation, and accuracy. This function ensures that encryption achieves both strong privacy protection and computational efficiency. This function can be defined as:

$$F \frac{[P+U+H+(1-I)+Ac]}{5}_{max} \quad (11)$$

where P denotes privacy, U utility, H hiding ratio, I information preservation, and Ac the accuracy of an MLP. The fitness function scores each key, guiding DES-SBOA to select the most secure and usable solution.

Privacy protects sensitive information from unauthorized access, ensuring confidentiality and preventing breaches [19].

$$P = \frac{1}{H \times I}\sum_{a=1}^{H}\sum_{b=1}^{I}\frac{(A_{ab}-A_{ab}^{*})}{Max(A_{ab},A_{ab}^{*})} \quad (12)$$

where A_{ab}^{*} depicts data elements of retrieved data, H is the total count of data holders or sources, and I is the number of data elements or instances being analyzed.

Utility balances privacy with data usability, ensuring transformed data remains meaningful for analysis, decision-making, and machine learning applications [20].

$$U = \frac{c+d}{2} \quad (13)$$

where c depicts the mean and d depicts the covariance.

The hiding ratio measures the proportion of data concealed during anonymization or encryption. Higher ratios improve security but may reduce usability, requiring a balance between privacy and functionality. It is defined as:

$$H = \frac{O}{U} \quad (14)$$

where the term O is the index length and U is the highest count of hidden data indexes.

Information preservation [21] ensures that the encrypted data retains the key statistical properties and distribution of the original data, maintaining its usefulness for analysis. It is defined as:

$$I = \frac{O_1}{V} \quad (15)$$

where V is the total number of indexes in preserved data and O_1 denotes the count of zero indexes.

Accuracy states the degree of correctness of processed data compared to the original data. Accuracy is expressed as:

$$Ac = \frac{TP+TN}{TP+TN+FP+FN} \quad (16)$$

where TP denotes True Positives, TN True Negatives, FP False Positives, and FN False Negatives. The accuracy of preserved data is examined using an MLP for secret key optimization to assess utility and accuracy in the fitness function. This MLP learns from both original and encrypted data to verify that encryption preserves data quality. High accuracy confirms that meaningful patterns remain useful for machine learning models while maintaining privacy. The MLP consists of input, hidden, and output layers, connected through nonlinear activation functions. The MLP is a universal approximator capable of modeling complex relationships, scalable for large datasets, and widely applied in classification and regression tasks [22].

$$\hat{u} = \varepsilon_0\left\{\sum_{z=1}^{c} L_{jg}^{o}\left[\varepsilon_e\left(\sum_{z=1}^{l} L_{jg}^{E} K_d\right)\right]\right\} \quad (17)$$

where, L_{jg}^{E} and L_{jg}^{o} denote the weights of the hidden and the output layers, and ε_e and ε_0 are the activation functions for the hidden and the output layers. K_d is a feature input at a sample time l, z represents the count of units in a hidden layer, and c is the overall count of hidden layers in MLP. Figure 4 shows the structural diagram of the MLP.

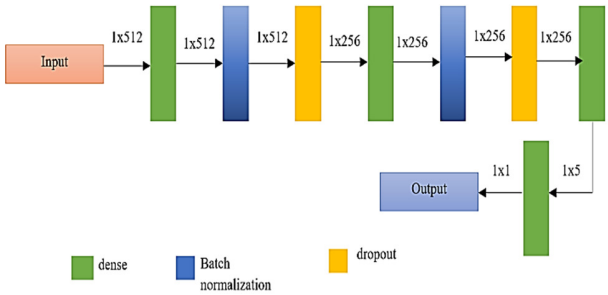


Fig. 4. Structural illustration of MLP.

SHA-256 ensures secure decryption and integrity. The user submits a hash of the secret key, which the cloud system verifies against the stored hash. If matched, data is decrypted; otherwise, access is denied [23].

$$BA^* = A^* \oplus r_{1\times q} \quad (18)$$

Once the correct encrypted data is obtained, it is decrypted using BFV with the retrieved secret key to restore the data as follows:

$$Rd = Decrypt(BA^*, C) \quad (19)$$

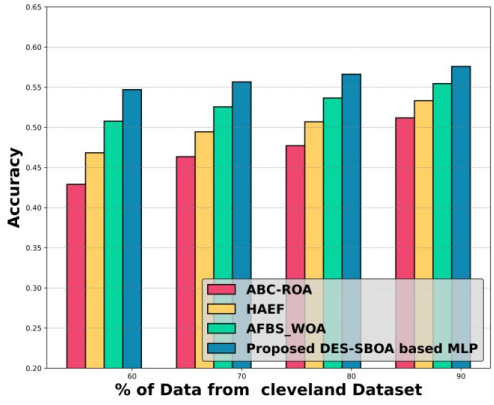
Since the SHA-256 hash functions are irreversible, it is only possible to produce a valid hash using the original key, and authentication is tamper-proof. This ensures confidentiality, authenticity, and integrity, and therefore SHA-256 is well-suited for privacy-sensitive areas, such as cloud-based data mining [24].

IV. RESULTS AND DISCUSSION

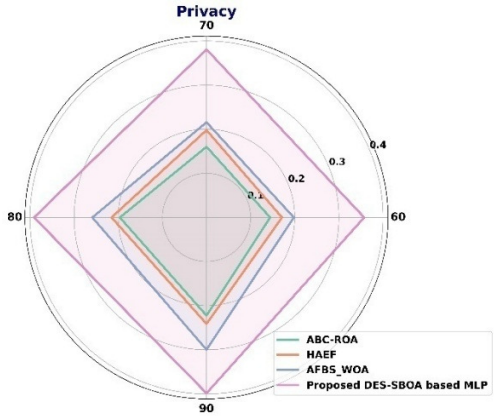
The Cleveland and VA Long Beach heart disease data is a collection of clinical data, including blood pressure, cholesterol, ECG, age, sex, and type of chest pain, along with a target variable that denotes the existence of heart disease [25]. These datasets were used to assess the proposed privacy-preserving data mining approach. Six indicators were used to evaluate the proposed approach, namely hiding ratio, information preservation, accuracy, privacy, utility, and execution time. The combination of these metrics evaluates privacy protection, retention of statistical properties, usability, and execution efficiency. The results on accuracy, privacy, utility, and execution time on the Cleveland and VA Long Beach datasets are compared in Figures 5 and 6.

Figure 5 offers a detailed comparative evaluation on the Cleveland data in four main dimensions, namely accuracy, privacy, utility, and execution time, for ABC-ROA, HAEF, AFBS-WOA, and the proposed DES-SBOA-based MLP model. As shown in Figure 5(a), the MLP in DES-SBOA has the highest classification accuracy in all data proportions (60-90%). The learning ability and the strength of the proposed method increase with training data, and the baseline models show relatively lower change in accuracy and slower learning.

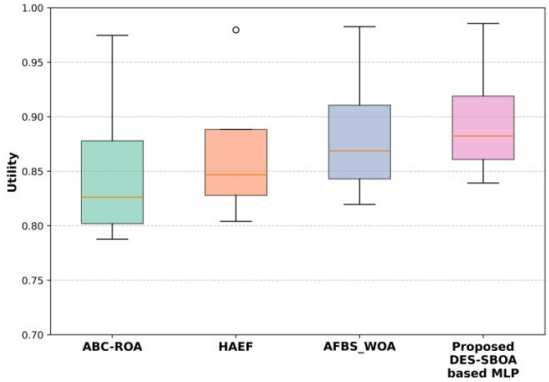
(a)



(b)



(c)



(d)

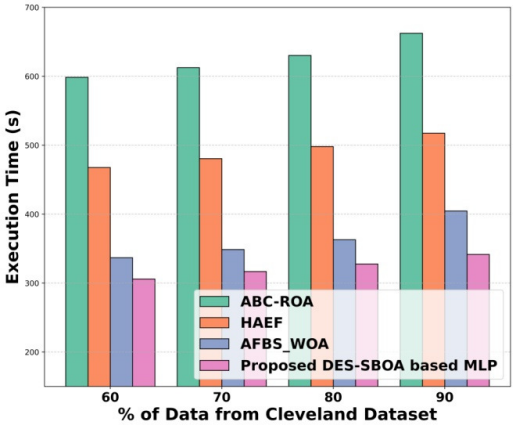


Fig. 5. Comparative examination on the Cleveland dataset: (a) Accuracy, (b) Privacy, (c) Utility, (d) Execution time.

Figure 5(b) shows that the proposed method has a better privacy-preservation property, which is suggestive of a better optimization of privacy-conscious constraints compared to the other methods. Figure 5(c) shows the analysis of utility, revealing that the proposed method has better median utility and less dispersion, demonstrating more consistent and reliable performance, whereas the median utility and range of dispersion are lower in ABC-ROA and HAEF. Lastly, Figure 5(d) emphasizes execution time, where the DES-SBOA-based MLP uses the lowest computation time in all training data sizes, hence establishing its computational efficiency and scalability.

Figure 6 provides a comparative performance analysis on the VA Long Beach dataset, assessing accuracy, privacy, utility, and the execution time of ABC-ROA, HAEF, AFBS-WOA, and the proposed DES-SBOA-based MLP. Figure 6(a) shows that the DES-SBOA-based MLP has the highest accuracy in all training data ratios (60-90%), thus presenting high learning competence and generalization with an increase in the volume of training data. Conversely, the rival approaches have lower absolute accuracies and slower enhancements. Figure 6(b) demonstrates that the DES-SBOA-based MLP has far higher privacy rates on all the data splits, implying that it has a better privacy-sensitive optimization capability compared to the baseline strategies. In Figure 6(c), the utility analysis shows that the DES-SBOA-based MLP has the largest median utility and the smallest dispersion, which indicates more consistent and credible performance. In comparison, the utility values of ABC-ROA, HAEF, and AFBS-WOA achieve relatively lower values and have a broader range of variability. Figure 6(d) indicates that the DES-SBOA-based MLP takes the shortest time to run with all data set sizes, demonstrating its efficiency and scalability in terms of computation.

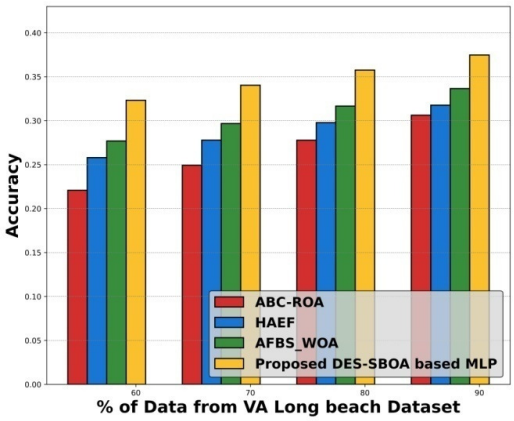
TABLE I. STATISTICAL ANALYSIS ON THE CLEVELAND DATASET

Method	ABC-ROA	HAEF	AFBS_WOA	Proposed DES-SBOA-based MLP
Best	0.569	0.582	0.606	0.629
Mean	0.534	0.565	0.586	0.617
Variance	0.034	0.017	0.019	0.012
Standard deviation	0.186	0.131	0.140	0.110

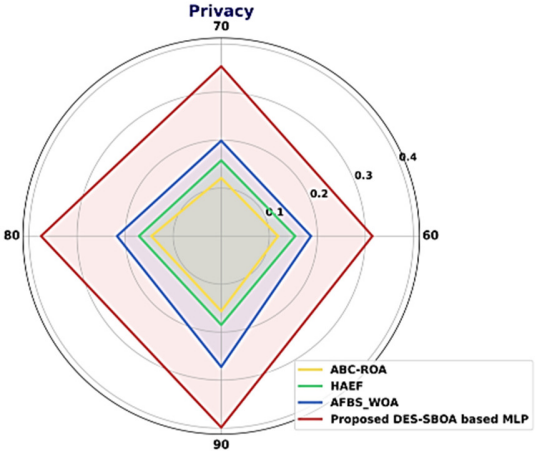
TABLE II. STATISTICAL ANALYSIS ON THE VA LONG BEACH DATASET

Method	ABC-ROA	HAEF	AFBS_WOA	Proposed DES-SBOA-based MLP
Best	0.566	0.572	0.598	0.614
Mean	0.502	0.525	0.553	0.578
Variance	0.064	0.047	0.045	0.036
Standard deviation	0.253	0.217	0.213	0.190

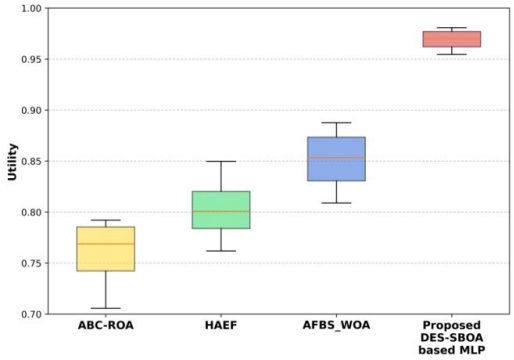
(a)



(b)



(c)



(d)

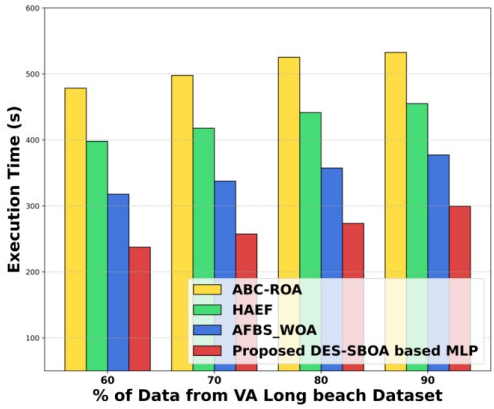


Fig. 6. Comparative examination on the VA Long Beach dataset: (a) Accuracy, (b) Privacy, (c) Utility, (d) Execution time.

Overall, the proposed DES-SBOA-based MLP performed better than the ABC-ROA, HAEF, and AFBS-WOA algorithms. For example, in 90% training data, the proposed model achieved accuracies of 0.576 on Cleveland and 0.575 on VA Long Beach, which are higher than the competing methods (0.555). Other performance areas, such as privacy, also improved to 0.399 and 0.398, respectively, a significantly higher score compared to the greatest competitor (0.300 and 0.299). Similarly, the utility in both datasets was higher than 0.98, whereas that of AFBS_WOA was 0.896. The execution time was also significantly lower, reducing to 48.5% compared to the alternatives.

Tables I and II demonstrate the statistical stability of the proposed method, as it produced the best and mean scores with the least variance and standard deviation, proving robustness. Finaly, Table III provides a summary of overall comparative performance, demonstrating improvements up to 17.4 in utility and 79.7 in privacy, which proves that the DES-SBOA-based MLP provides a better balance between privacy, accuracy, and efficiency.

TABLE III. MODEL COMPARISON

Method	ABC-ROA	HAEF	AFBS_WOA	Proposed DES-SBOA-based MLP
Accuracy	0.511	0.533	0.554	0.575
Privacy	0.222	0.241	0.299	0.398
Utility	0.839	0.868	0.896	0.985
Fitness	0.569	0.582	0.606	0.629
Execution time (s)	662.3	517.4	404.5	341.5

V. CONCLUSION

This study presents a privacy-preserving method for optimizing deep learning performance in protected data mining, offering a powerful cloud data encryption and retrieval system. Data preservation was ensured using BFV homomorphic encryption, where the original data was encrypted with a secret key and manipulated with a random matrix to provide an additional layer of security. Key optimization was performed using the DES-SBOA algorithm, which incorporated DES into SBOA. In this optimization algorithm, the fitness function was used to assess various candidate keys based on weighted privacy, utility, hiding ratio, information preservation, and accuracy. After encryption, the data was stored in the cloud. During data recovery, the user provided a hash of the secret key to verify the user, and once this was done, the data were reconstructed using the key.

The proposed method achieved an accuracy of 57.5, privacy of 39.8, utility of 98.5, fitness of 62.9, and execution time of 341.5 s. Future work should examine the improvement of privacy-preserving DL models by incorporating hybrid deep learning and differential privacy methods to achieve more robust and secure data mining. The study of new encryption techniques and optimization methods might enhance efficiency and scalability. In contrast to other privacy-sensitive data mining methods (ABC-ROA, HAEF, and AFBS_WOA), the proposed framework offers a new combination of BFV homomorphic encryption with a temporally stabilized meta-heuristic optimization algorithm (DES-SBOA). The main innovation is the use of DES in the SBOA process, which improves its convergence stability and reduces early stagnation when generating secret keys—something that previous research has not yet covered.

The proposed method enables arithmetic operations on encrypted data, which are performed securely, without the need for decryption before analysis, as opposed to the ABC-ROA or AFBS_WOA, which optimize keys without taking into account the temporal trends and encrypted domain computation. Unlike HAEF-based anonymization methods that undermine privacy in favor of usability under dynamic publishing conditions, the proposed method maintains statistical integrity and utility (0.985) and achieves considerably better privacy scores (0.398). In addition, the use of an MLP-based error measure in the fitness function offers a statistical confirmation of utility preservation, which, again, is surprisingly missing in previous heuristic-only models.

REFERENCES

[1] M. Kumar *et al.*, "A smart privacy preserving framework for industrial IoT using hybrid meta-heuristic algorithm," *Scientific Reports*, vol. 13, no. 1, Apr. 2023, Art. no. 5372, https://doi.org/10.1038/s41598-023-32098-2.

[2] Z. Tang, M. Ye, Y. Liu, and S. Wei, "Privacy-Preserving Multimedia Mobile Cloud Computing Using Protective Perturbation." arXiv, Sept. 03, 2024, https://doi.org/10.48550/arXiv.2409.01710.

[3] R. Mendes and J. P. Vilela, "Privacy-Preserving Data Mining: Methods, Metrics, and Applications," *IEEE Access*, vol. 5, pp. 10562–10582, 2017, https://doi.org/10.1109/ACCESS.2017.2706947.

[4] Y. S. Hindistan and E. F. Yetkin, "A Hybrid Approach With GAN and DP for Privacy Preservation of IIoT Data," *IEEE Access*, vol. 11, pp. 5837–5849, 2023, https://doi.org/10.1109/ACCESS.2023.3235969.

[5] Y. V. R. S. Viswanadham, and K. Jayavel, "A Framework for Data Privacy Preserving in Supply Chain Management Using Hybrid Meta-Heuristic Algorithm with Ethereum Blockchain Technology," *Electronics*, vol. 12, no. 6, Mar. 2023, https://doi.org/10.3390/electronics12061404.

[6] L. Xu, X. Cheng, W. Tian, H. Wang, and Y. Zhang, "Cloud-Assisted Privacy-Preserving Spectral Clustering Algorithm Within a Multi-User Setting," *IEEE Access*, vol. 12, pp. 75965–75982, 2024, https://doi.org/10.1109/ACCESS.2024.3404265.

[7] Z. Tang, M. Ye, Y. Liu, and S. Wei, "Privacy-Preserving Multimedia Mobile Cloud Computing Using Protective Perturbation." arXiv, 2024, https://doi.org/10.48550/ARXIV.2409.01710.

[8] A. Ali *et al.*, "HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications," *Sensors*, vol. 23, no. 15, July 2023, https://doi.org/10.3390/s23156762.

[9] S. T. Revathi, A. Gayathri, J. Kalaivani, M. S. Christo, D. Pelusi, and M. Azees, "Cloud-Assisted Privacy-Preserving Method for Healthcare Using Adaptive Fractional Brain Storm Integrated Whale Optimization Algorithm," *Security and Communication Networks*, vol. 2021, no. 1, 2021, Art. no. 6210054, https://doi.org/10.1155/2021/6210054.

[10] A. Majeed and S. Lee, "Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 8512–8545, 2021, https://doi.org/10.1109/ACCESS.2020.3045700.

[11] E. Hesamifard, H. Takabi, M. Ghasemi, and R. N. Wright, "Privacy-preserving Machine Learning as a Service," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 3, pp. 123–142, June 2018, https://doi.org/10.1515/popets-2018-0024.

[12] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *Proceedings of the 2000 ACM SIGMOD International Conference on*

Management of Data, Dallas, TX, USA, May 2000, pp. 439–450, https://doi.org/10.1145/342009.335438.

[13] T. Hunt, C. Song, R. Shokri, V. Shmatikov, and E. Witchel, "Chiron: Privacy-preserving Machine Learning as a Service." arXiv, Mar. 15, 2018, https://doi.org/10.48550/arXiv.1803.05961.

[14] M. A. Sahi *et al.*, "Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions," *IEEE Access*, vol. 6, pp. 464–478, 2018, https://doi.org/10.1109/ACCESS.2017.2767561.

[15] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, "Tools for privacy preserving distributed data mining," ACM *SIGKDD Explorations Newsletter*, vol. 4, no. 2, pp. 28–34, Sept. 2002, https://doi.org/10.1145/772862.772867.

[16] S. Alabdulwahab, Y.-T. Kim, Y. Son, S. Alabdulwahab, Y.-T. Kim, and Y. Son, "Privacy-Preserving Synthetic Data Generation Method for IoT-Sensor Network IDS Using CTGAN," *Sensors*, vol. 24, no. 22, Nov. 2024, https://doi.org/10.3390/s24227389.

[17] N. Narula, W. Vasquez, and M. Virza, "zkLedger: Privacy-Preserving Auditing for Distributed Ledgers," presented at the 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18), 2018, pp. 65–80.

[18] H. Vaghashia and A. Ganatra, "A survey: privacy preservation techniques in data mining," *International Journal of Computer Applications*, vol. 119, no. 4, pp. 20–26, 2015.

[19] Y. A. A. S. Aldeen, M. Salleh, and M. A. Razzaque, "A comprehensive review on privacy preserving data mining," *SpringerPlus*, vol. 4, no. 1, Nov. 2015, Art. no. 694, https://doi.org/10.1186/s40064-015-1481-x.

[20] H. Chabanne, A. de Wargny, J. Milgram, C. Morel, and E. Prouff, "Privacy-Preserving Classification on Deep Neural Network." Cryptology ePrint Archive, 2017.

[21] K. Bonawitz *et al.*, "Practical Secure Aggregation for Privacy-Preserving Machine Learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Dallas, TX, USA, July 2017, pp. 1175–1191, https://doi.org/10.1145/3133956.3133982.

[22] J. J. LaViola, "Double exponential smoothing: an alternative to Kalman filter-based predictive tracking," in *Proceedings of the workshop on Virtual environments 2003*, Zurich, Switzerland, Feb. 2003, pp. 199–206, https://doi.org/10.1145/769953.769976.

[23] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a New Model to Secure IoT-based Smart Home Mobile Agents using Blockchain Technology," *Engineering, Technology & Applied Science Research*, vol. 10, no. 2, pp. 5441–5447, Apr. 2020, https://doi.org/10.48084/etasr.3394.

[24] H. Taud and J. F. Mas, "Multilayer Perceptron (MLP)," in *Geomatic Approaches for Modeling Land Change Scenarios*, M. T. Camacho Olmedo, M. Paegelow, J.-F. Mas, and F. Escobar, Eds. Springer International Publishing, 2018, pp. 451–455.

[25] W. S. A. Janosi, W. Steinburn, M. Pfisterer, and R. Detrano, "Heart Disease." UCI Machine Learning Repository, 1989, https://doi.org/10.24432/C52P4X.