Applied Data Science and Analysis
Vol.2025, **pp**. 155–164
DOI: https://doi.org/10.58496/ADSA/2025/013 ; ISSN: 3005-317X
https://mesopotamian.press/journals/index.php/ADSA

Research Article

Strengthening cloud data protection based on a novel cyber security framework

Ammar Mhana [1,*], Fadhel K. Jabor [2], Ghufran A. Omran [2], Jamal Fadhil Tawfeq [3], Ahmed Dheyaa Radhi [4], Varsha K. Harpale [5], Mrinal Bachute [6], Pritesh Shah [6], Ravi Sekhar [6]

[1] College of the Science, University of Baghdad Baghdad, Iraq.

[2] Vice President Office for Scientific Affairs, University of Baghdad, Baghdad, Iraq.

[3] Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi University, Baghdad 00965, Iraq

[4] *College of Pharmacy, University of Al-Ameed, Karbala PO Box 198, Iraq*

[5] Department of Electronics and Telecommunications, Pimpri Chinchwad College of Engineering, Pune-44, India.

[6] Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University) (SIU), Pune 412115, Maharashtra, India

ARTICLE INFO

Article History

Received 14 Feb 2025
Revised: 15 Mar 2025
Accepted 10 Apr 2025
Published 01 May 2025

Keywords

Cloud Data Protection
Cyber Security Framework
Intrusion Detection
Dung Beetle optimization-redefined Intelligent Random Forest (DB-IRF).

ABSTRACT

Cybersecurity involves protecting computer networks, systems, and data from unauthorized access and disruptions using advanced technologies. The purpose of this research is to establish a novel cyber security framework for strengthening cloud data protection. In this paper, we propose a novel Dung Beetle optimization-redefined Intelligent Random Forest (DB-IRF) for accurate detection of intrusions in a cloud environment. We obtained a dataset that includes cloud system logs and network traffic data, including normal and malicious activities, to train our proposed model. We utilized z-score normalization to pre-process the gathered raw data. Our suggested model enhances classification accuracy by integrating DB optimization with the IRF algorithm. It optimizes feature importance weights during training and improves the model's ability to detect intrusions in cloud environments accurately. The proposed detection model is implemented in Python software. In the findings assessment phase, we effectively assessed the performance of our proposed DB-IRF in detecting earthquake incidents across multiple evaluation metrics such as Accuracy (97.5%), Precision (97.96%), F1 Score (98.48%) and Recall (97.85%). We also conducted a comparison analysis with other conventional methodologies. Our experimental results demonstrate the capability and reliability of the recommended framework.

1. INTRODUCTION

Introduction of security measures and practices that are essential to reduce risks arising from cyber-attacks, unauthorized access, and information breaches for cloud data. Among all, encryption is crucial to ensure cloud data security [1]. Digital information is the crucial component of any business globally; thus, guaranteeing security became mandatory while uploading on the cloud platforms. They shield confidential information against attacks of cybersecurity while also improving company operations over the cloud [2]. The concepts of cybersecurity help in the protection of data that may be stored, processed, or transferred over a cloud infrastructure-this provides the field with the name 'cloud data protection'. The approach of cryptography did further provide an extended level of protection in personal data ownership [3]. Other major factors of effective cloud data security include robust access restrictions and verification processes. Multi-factor authentication is applied in these systems, ensuring that the authorized user gains access to confidential information whose identities have already been verified [4]. The use of cryptography, access control systems, monitoring, and threat detection is essential in the protection of information within the cloud. Machine learning methods and enhanced security insight will allow an organization to quickly notice and rectify problematic activity [5]. Organizations can detect anomalies and potential security incidents to take proactive measures in minimizing risks that may lead to data leakage or breach [6]. Cloud architectures are dynamic, adaptable, aggressive, and flexible approaches that make up cybersecurity. Traditional static security solutions often fail to keep pace with the changing nature of the threat landscape. Also, compliance with business standards and legal regulations was necessary to ensure cloud data security. Hazardous information security was

*Corresponding author. Email: ammar.mhana@uobaghdad.edu.iq

governed by strict rules in several areas, including health care, government and banking. Cloud service providers are required to follow security procedures to ensure. Data recovery and backup planning are the components of cloud security [7]. The natural catastrophes and security breaches, companies need to constitute backup strategies for recovering data and continuing operations. Organizations may reduce the effect of interruptions and guarantee uninterrupted operations by constantly backing up data to distributed sites and putting robust disaster recovery policies [8]. The study aim is to develop digital infrastructure for cloud data protection that protects the security, accessibility and reliability of data stored in a cloud environment. We propose a novel Dung Beetle optimization-redefined Intelligent Random Forest (DB-IRF) for accurate detection of intrusions in a cloud environment. Most of the existing cybersecurity frameworks for cloud data protection lack dynamic adaptation to the ever-changing threat landscape, robustness in anomaly detection, and accuracy in classifying malicious activities in the cloud environment. Most of the traditional approaches are based on static security mechanisms that are incompetent against evolving cyber threats and also fail to optimize the trade-off between detection accuracy and computational efficiency. Approaches based on K-Nearest Neighbors, Gaussian Naïve Bayes, and Support Vector Machines all have their different weaknesses when handling diverse and high-dimensional datasets, hence doing intrusion detection below par. The proposed DB-IRF framework fills the gaps by adopting a hybrid approach that combines the dynamic optimization capabilities of the Dung Beetle algorithm with the robust classification accuracy of the Intelligent Random Forest (IRF). This allows the framework to enhance feature importance weighting and optimize resource allocation dynamically, leading to better anomaly detection and intrusion prevention in cloud environments. The proposed DB-IRF framework has been validated through experimental results, with remarkable improvements in performance: 97.5% accuracy, 97.96% precision, 98.48% recall, and 97.85% F1-score, outperforming traditional methods, thus proving to be reliable and efficient in enhancing the protection of cloud data.

The following Sections make up the article: Section 2, Literature Review; Section 3, Methodological part; Section 4, Experimental result; and Section 5, Conclusion.

2. RELATED WORKS

Enhancing the quantity of CTI accessible for assessment facilitates enhanced anticipation, avoidance and alleviation of cyberattacks [9]. The CTI information was altered before releasing for assessment, the information possessor can select the right degree of security and CTI information hygiene technique that includes simple text and homomorphic cryptography. Theoutcome of the experiment leads to several implementations to analyze CTI information in the cloud.The data protection integrates SE with memory fragment and diffusion. The data protection was divided into three distinct levels of security by convertible DWT. They are distributed among several locations for storage with varying degrees of reliability to safeguard end users' data by resisting potential cloud breaches.The experimental findings demonstrate that a high degree of security constitutes resistant faults in replication. Mobile operator architecture was used to implement the dispersed virtualization operator paradigm in the cloud [10,11]. Multi-tenants constitute together to verify the integrity of data with a virtualization operator. The role of the virtualization operator function was accomplished to dependable storage of information, tracking and authentication. The experimental outcome demonstrates the utilization of dispersed virtualization gateway model deployment in a cloud environment. They examined AuthPrivacy-Chain, a blockchain technology system for access control that safeguards privacy. The permissions for controlling access to cloud-based information were secured and stored in block chain technology by using the node's identity information [12]. AuthPrivacy-Chain was implemented by using EOS. The outcome of the experiment indicates that assets can be accessed by authorized users. Research examined a cloud-based safe information security approach that offers cloud security problems, including safeguarding information from intrusions and defense against a phony authorized identity user compromises cloud security [13]. They develop OTP for tracking and exporting methods to safeguard data and user individuals against any fraudulent or unethical use of the cloud. The experimental outcome demonstrates that the suggested approach offered the advantages and efficiency of cloud computing security.The PIPA would leverage cloud computing to identify files containing sensitive data and notify the relevant individuals [14]. The Hadoop distributed computing platform was utilized to facilitate the processing of enormous volumes of data.The results of the experiments demonstrated the suggested Hadoop system efficiently increased the speed of execution. The non-commutative encryption framework constitutes a Quantum Key Distribution (QKD) [15]. The QKD ensures highly secure data transfer. Furthermore, guarantee protected key creation with decreased time complexitywas produced. The experimental outcome demonstrates that security risks constitute ensuring secure information transport and storage at lower computation. Most of the IDSs in cloud environments are suffering from significant limitations that curtail their effectiveness in addressing dynamic and evolving cybersecurity challenges of modern cloud platforms. Traditional IDSs rely on static detection methods, such as signature-based approaches, which are ineffective in detecting novel or zero-day attacks. These systems also face difficulties in balancing the rates of false positives and false negative cases, with a lot of superfluous alerts or missing detections that reduce reliability and operational efficiency. Scalability is another important concern: classic IDSs were not designed to

cope with the volume, velocity, and variety of data produced within cloud environments; hence, the detection and response will be much slower. Secondly, many of them are missing some advanced optimized features that tend to give priority to data relevance detection; the accuracy remains reduced while computations become higher. Detection capability is unsatisfactory; in most IDS, detection depends upon patterns of attack traffic and therefore usually fails while facing sophisticated or unpredictable threats. Thirdly, conventional IDSs have been seen to be computationally heavy and often not adapted to resource-starved cloud platforms. The proposed framework, Dung Beetle optimization-redefined Intelligent Random Forest, overcomes these lacunae by incorporating the Dung Beetle Optimization algorithm into the Intelligent Random Forest methodology. This hybrid approach contributes to an immense enhancement in feature importance weighting and optimizes resource allocation to adapt dynamically to the evolution of threats dynamically. The proposed framework of DB-IRF tends to achieve superiority in intrusion detection accuracy with substantial reduction in false positives and negatives. It has a scalable design that can manage large and heterogeneous datasets. Its advanced anomaly detection allows it to identify novel threats in real time. It minimizes computational demands by focusing on relevant features, thus making it suitable for resource-constrained cloud environments. These innovations make the DB-IRF framework a robust and effective solution to the shortcomings of existing IDSs, ensuring enhanced security and reliability in cloud platforms.

3. METHIODOLOGY

Figure 1 presents the proposed methodology. We have collected a dataset from Kaggle. We used z-score normalization for the pre-processing of raw data. Further, we have proposed a new metaheuristic optimization-based Dung Beetle-redefined Intelligent Random Forest (DBIRF) for accurate detection of intrusions in the cloud environment.

3.1 Data pre-processing using Z-Score normalization

The quantity of standard errors was represented by Z-Score, a traditional normalization and standardization technique that indicates the raw data value constitutes the overall population mean. It was optimally located among -3 and +3. The dataset was normalized to the previously indicated scale data with various dimensions. The z-score is a tool used to stabilize information. To calculate the rating, eliminate the overall population average from an unprocessed data point and divide the result by the standard deviation of the data. The result ideally ranges from -3 to +3, indicating the number of standard deviations that a point deviates from the mean was determined in Equation (1), where y stands for the median value of a specific samples, μ for the median, and σ for the average variation.

$$Z\_Score = \frac{(y-\mu)}{\sigma} \tag{1}$$

Z:Z-score
X : Data point value
μ : Mean of the dataset
σ : Standard deviation of the dataset

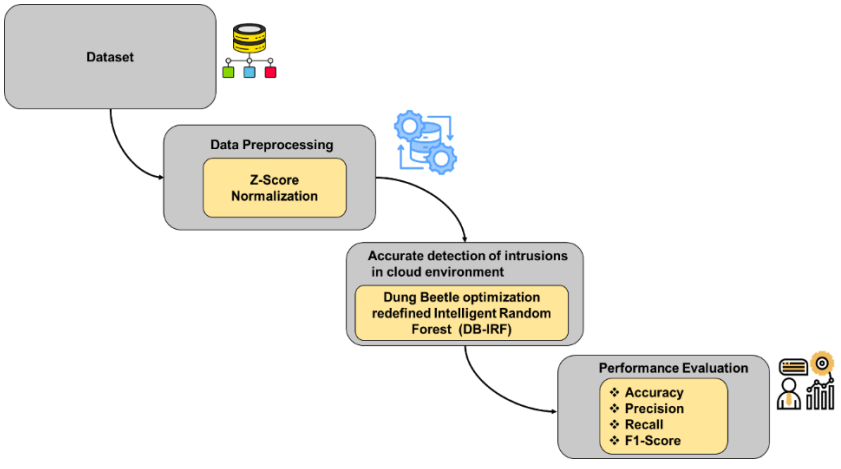

Fig. 1. Proposed Methodology

3.2 Dung Beetle Optimization (DB)

Dugout beetle behaviors including slipping, humming foraging, pillaging and reproducing are the source of inspiration for the dung beetle technique. On the basis of these behaviors, four population rejuvenation techniques are developed.
Equation (2) describes the behavior of dung beetles and continuously updates their location in sunlight based on environmental conditions including wind direction and sunshine.

$$y_j(s+1) = y_j(s) + \propto \times l \times y_j(s+1) + a \times \Delta y, \quad \Delta y = \left| y_j(s) - Y^{\omega} \right| \tag{2}$$

$y_j(s)$: The position or location of dung beetle j at iteration R.
& The current iteration number ar quantity.
a: A direction factor of chung beetles, with values between 1 and -1 where
$\alpha = 0$. No direction difference.
$\alpha = -1$: Indicates deviation.
I: A random integer within the range (0,2).
Δy. The change in position, defined as the absolute difference between $y_j(s)$ the current position) and y^{ρ} (the worldwide lowest location).
y^b : The worldwide lowest position or location.
l : The deflection factor, a parameter used to simulate environmental influences like light. $l \in (0,0.3)$.

The variables $s$and $y_j(s)$represent the current iteration quantity and the location of j represents the dung beetle during s repetition, respectively. a represents the direction of dung beetles varies and its value set between 1 and −1. Where 1 indicates no difference and −1 indicates a deviation. Y^{ω}indicates the worldwide lowest location, $\Delta y$was utilized to mimic the light quantity, and l∈ (0, 0.3) as the deflection factor. $a$indicates an integer that raises from (0,2).The dung beetles will run into obstacles and likely find a new path. Equation (3) describes this dancing behavior.

$$y_j(s+1) = w_j(s) + \tan(\theta) \left| y_j(s) - y_j(s-1) \right| \tag{3}$$

$H_j(s+1)$: The new location of dung beetle j at the next iteration.
$w_j(s)$: The weight or influence of sunlight at iteration s.
θ : Angle of deviation, which influences the dung beetle's behavior. The location remains unchanged if $\theta \in \left[-\frac{\pi}{2}, \pi\right]$.
$\left| y_j(s) - y_j(s-1) \right|$: The absolute difference in position between the current and previous iterations. The dung beetle's location will remain unchanged when θ is between $\frac{\pi}{2}$and π for $\theta \in [0, \pi]$. Dugout beetles reproduce in safe areas and characterized by threshold selection strategies represented in Equation (4), to ensure a secure habitat for their progeny.

$$Q = 1 - s/S_{max}, \quad Lb^* = \max(W^* \times (1-Q), Lb), \quad Ub^* = \min(W^* \times (1-Q), Ub) \tag{4}$$

Lb' : The lawer boundary for the spawning region.
Ub' ' The upper boundary for the spawning region.
W^* : The aptimal location for dung beetles.
Q: A corvergence rate factor calculated $as = 1 - s/\kappa_{\text{musx}}$, where:
k Current iteration.
B_{maxx} : Maximum number of iterations.
Lb: Original lower boundary of the region.
Ub: Original upper boundary of the region.

Where Y^* indicates the optimal location, S_{max}stands for the maximum amount of iterations, $Q$for the rate of convergence factor,Lb^* and $Ub^*$for the bottom and top borders of the spawning region, and $Lb$and$Ub$for the upper and lower limits. Equation (4) indicates the spawning region was determined by the quantity of Qeffectively; hence, the position of the deposited embryos likewise interactively altered. Equation (5) represents the hatching region.

$$A_j(s+1) = Y^* + a_1 \times \left(A_j(s) - Lb^*\right) + a_2 \times \left(A_j(s) - Ub^*\right) \tag{5}$$

$A_j(s+1)$: The position of the j-th reproductive ball at the next iteration.

Y^* : The optimal location for reproduction.
a_1, a_2 : Randomized coefficients for direction and influence, which simulate random movement or dispersion.
$A_j(s)$: The current position of the f-th reproductive ball.
Lb^* : Updated lower boundary of the spawning region (from Equation 4)-
Ubr': Updated upper boundary of the spawning region (from Equation 4).

Where a_1 and a_2 represent distinct randomized vectors and w indicates two variables that perform element-wise addition, and $A_j(s)$indicates the position of the j^{th} reproductive ball in s th repetition.
The optimum place to graze, immature dung beetles must first determine its boundaries, which was determined by Equation (6).

$$Lb^a = \max\left(Y^a \times (1-Q), Lb\right)$$
$$Ub^a = \min\left(Y^a \times (1+Q), Ub\right) \quad (6)$$

Lb^2 : Lower bound of the optimal foraging area.
UV^2 : Upper bound of the optimal foraging area
Y^* : Glabal optimal position.
Q: A parameter that defines the range of the search space
Lb and Ubx The initial lower and upper bounds.

When the global optimum location was shown by Y^a, the bottom and top boundaries of the optimal foraging area were indicated by the $Lb^a$and Ub^a sub-tables. Equation (7) illustrates the little dung beetle's positional adjustment.

$$y_j(s+1) = y_j(s) + D_1 \times \left(y_j(s) - Lb^a\right) + D_2 \times \left(y_j(s) - Ub^a\right) \quad (7)$$

$y_j(s)$: Position of the coung beetle at iteration s.
$y_j(s+1)$: Updated position at the next iteration.
D_1 : An integer representing randomness following an average distribution.
D_2: A randomized vector within the range (0,2).
Lb^e and Ub^2 - Lower and upper bounds from Equation (6). Where D_2indicates a randomized vector and part of (0,2), and D_1 represents an integer of randomness that follows an average distribution.

The act of stealing was equivalent to robbing dung beetles of their dung balls. Equation (8) represents the thief dung beetle's geographic data updating approach during the repetitive phase.

$$y_j(s+1) = y^a + T \times h \times \left(\left|y_j(s) - Y^*\right| + \left|y_j(s) - Y^a\right|\right) \quad (8)$$

$y_j(s)$: Position of the thief dung beetle at iteration s.
$y_j(s+1)$: Updated position at the next iteration.
Y^* : A reference optimal position.
Y^a : Global optimal position.
T : A tuning parameter.
h : A scaling factor.

Where h represents a randomized vector of dimension that follows an average distribution and T stands for a fixed value.

3.3 Intelligent Random Forest (IRF)

The collection of decision trees was incorporated during every repetitive phase, the less relevant features were removed, and the performance of the classifier was monitored by IRF. To classify binary information, the RF approach was applied. During the learning phase, IRF builds several decision trees with average prediction models. Every hyper feature of the RF approach was imprinted by an organized search technique. The remaining variables are as follows: 2 minimum leaflet size; 4 minimum splitting size. The parameter values are: maximum randomized forests: 1000; maximum complexity: 10; assurance: 0.5; conviction: 0.5 in voting technique; Maximum imperfection; chopping; and prior pruning. Other settings are as follows: minimum leaflet size: 2, minimum splitting size: 4. Where Equation (9) was utilized in the IRF technique to compute a Relative distortion. Here, m represents the number of classifications utilized in the procedure and RP represents the probability of picking component features from the classification j information.

$$Gini_{Impurity} = \sum_{l=0}^{m} RP\left(j_{pc}\right)\left(1 - RP\left(j_{pc}\right)\right) \quad (9)$$

In the IRF technique, many decision trees function as a collective composition. Less computing expense and minimum decision trees constrained with characteristics may be constructed by the IRF approach. By averaging or perhaps a substantial proportion of vote, they combine several little decision-tree topologies into strong candidate like big tree structures. The most effective learning and instruction technique available in the IRF method.

3.4 Dung Beetle optimization-redefined Intelligent Random Forest (DB-IRF)

The hybrid strategy that combines the Intelligent Random Forest (IRF) and Dung Beetle Optimization (DBO) algorithms has surfaced as a reliable remedy for cloud data safety. The hybrid strategy offers increased resilience against cyberattacks by utilizing the dynamic learning potential of IRF in conjunction with DBO's natural ability to handle complicated situations and optimize the distribution of resources. Through the utilization of the strategies' combined intelligence, the infrastructure able to discover possible weaknesses, modify security measures in real-time, and improve the detection of anomalies, that helps to strengthen cloud computing platforms against cyber threats. The combination of computational learning and optimization methods (DB-IRF) inspired by the environment provides a strong defense, enabling businesses to protect the privacy and accuracy of data in the digital environment.

4. EXPERIMENTAL RESULTS

Initially, we obtained a dataset from Kaggle [16] that includes cloud system logs and network traffic data, including normal and malicious activities, to train our proposed model. Tensorflow1.12.0 was utilized to carry out the suggested work and accelerated by Nvidia GPUs. To complete the process, software must be installed in addition to Python. We assess the proposed approach and calculate the effectiveness of the strategy using the subsequent indicators: F1-score (%), Recall (%), Precision (%) and Accuracy (%). We also compare the effectiveness of our suggested technique with other existing methods. The current techniques consist of KNN [17], GNB [18] and SVM [19]. Table 1 illustrates the result parameters. Accuracy provides a strong assessment of the system's effectiveness by evaluating the model's preciseness assessment by computing the ratio of anticipated occurrences to the total occurrences. Figure 2 shows the comparative analysis for accuracy among the strategies methods and conventional techniques. Compared to current techniques such as KNN, GNB and SVM constitute accuracy 96.67%, 78.07%, and 97% and the suggested DB-IRF achieve a degree of specificity of 97.5%. Our suggested approach demonstrates superior outcomes for the detection of intrusions in cloud settings [19-28].

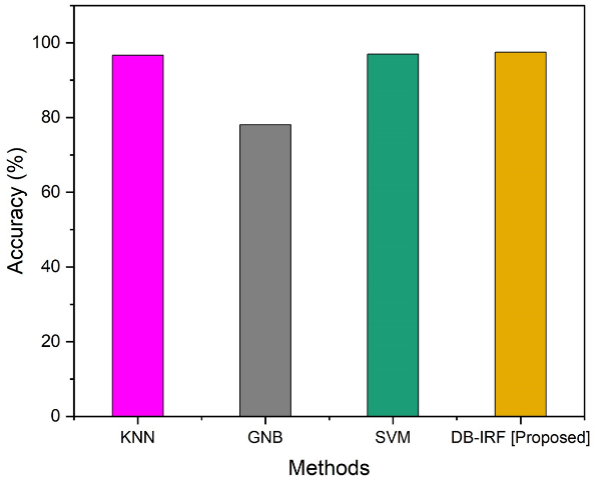

Fig. 2. Outcome of Accuracy

The accuracy of a model's predicted outcomes was determined through its level of precision. The ratio for precisely forecasting favorable findings with the total number of predicted benefits are evaluated.Figure 3 presents a comparative analysis of Precision among the strategies methods and conventional techniques. Compared to current techniques such as KNN, GNB and SVM among Precision of 97.51%, 85.53% and 96.23% and suggested DB-IRF attain a Precision of 97.96%. Our proposed method provided the efficiency of accurate detection of intrusions in a cloud environment.

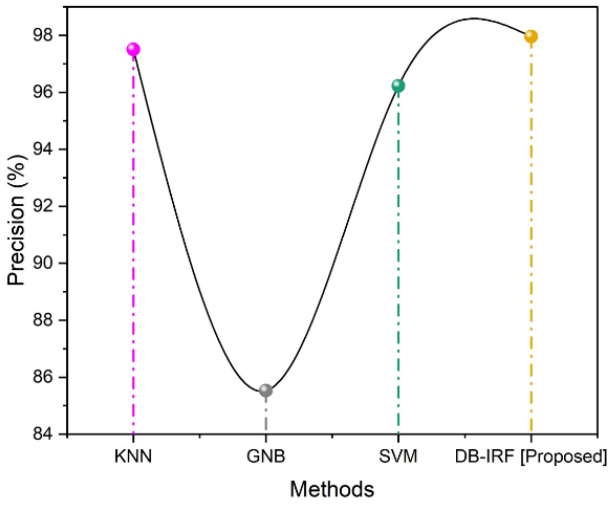

Fig. 3. Outcome of Precision

Recall measures the system's ability to capture all relevant hand movement instances and defined by the percentage of accurately anticipated positive cases compared to the total number of real positive cases.Figure 4 presents a comparative evaluation of the recall among the strategies methods and conventional techniques. Compared to current techniques such as KNN, GNB and SVM constitute recall 96.41%, 72.43% and 98.41% and the suggested DB-IRF attains a Recall of 98.48%. Our proposed method provided a superior outcome for the detection of intrusions in the cloud environment.

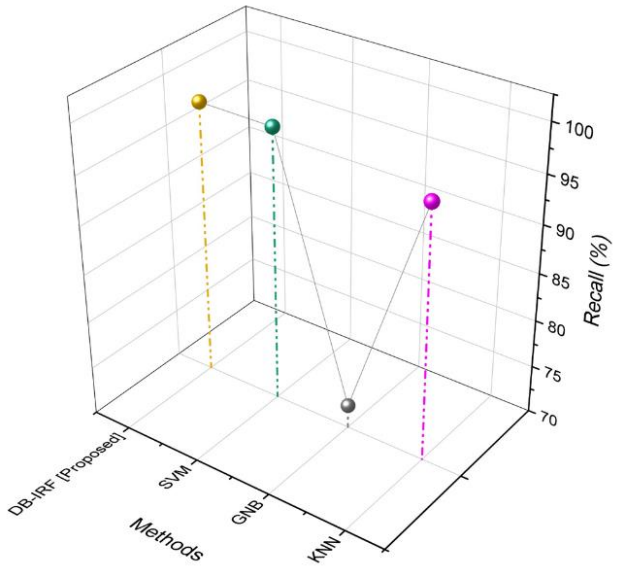

Fig. 4. Outcome of Recall

The harmonic mean of remembrance and accuracy is F1 score. It provides harmony between recollection and accuracy. Figure 5 presents a comparative analysis of F1-Score between the approach and traditional methods. In contrast to various methods such as KNN, GNB and SVM with F1-Score of 96.96%, 78.43% and 97.3% and the suggested DB-IRF attains an F1-Score of 97.85%. Our proposed method provided accurate detection of intrusions in a cloud environment.

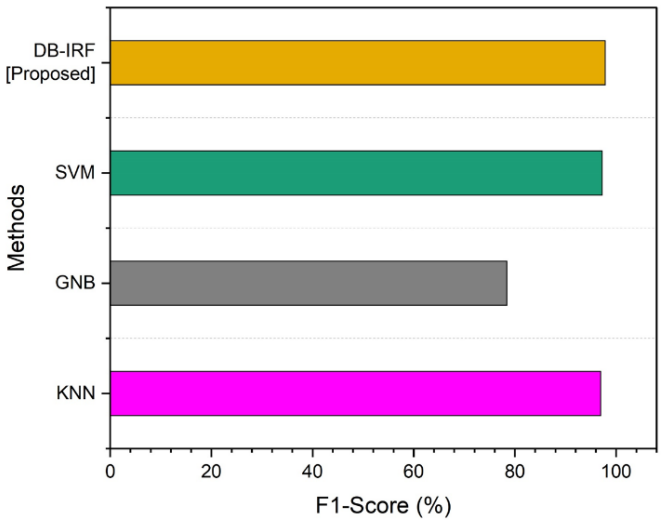

Fig. 5. Outcome of F1-Score

TABLE I. RESULTS PARAMETERS

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
KNN	96.67	97.51	96.41	96.96
GNB	78.07	85.53	72.43	78.43
SVM	97	96.23	98.41	97.3
DB-IRF [Proposed]	97.5	97.96	98.48	97.85

These results indeed prove that the proposed DB-IRF model outperforms all other traditional classification methods, such as K-Nearest Neighbors, Gaussian Naïve Bayes, and Support Vector Machines, in terms of accuracy, robustness, and efficiency. DB-IRF adopts a deep learning-based approach with integrated intelligent feature selection and rule-based classification, hence resulting in better decision-making capabilities, especially for high-dimensional and complex datasets. In contrast, KNN, though simple and effective on small datasets, is far from scalable and computationally efficient, since it degrades in performance with large volumes of data due to its reliance on distance-based calculations. GNB, though computationally efficient and theoretically optimal in the case of normally distributed data, suffers from independence assumptions that are hardly ever met in real-world cloud security datasets, hence yielding suboptimal classification accuracy. While on the other hand, SVM provides a strong generalization capability, mainly based on kernel-based transformations, which has a very high computational cost and is also unable to bear noisy data; hence, it cannot work perfectly for large-scale dynamic cloud environments. DB-IRF extends these by including deep learning-based feature extraction together with intelligent rule filtering to offer more adaptive and accurate classification mechanisms. Moreover, its automatic learning of complex feature interactions provides it with an edge over the usual machine learning process, which rests on manually designed representations of features. These results substantiate the efficacy of DB-IRF in enhancing data security in the cloud and its potentially high value for application in real-life cybersecurity.

5. CONCLUSION

From this research, it is noted that the DB-IRF framework outperforms most other approaches in the ability to provide accurate adaptive and efficient classification of security threats for better cloud data protection. In comparison with other classic approaches of machine learning methods such as KNN, GNB, and SVM, DB-IRF constitutes scalable robustness against noise and superior handling of high dimensionalities, being quite effective for modern cloud security applications. DB-IRF combines deep learning-driven feature extraction with rule-based decision-making, thus enabling it to automatically learn complex patterns and interactions in cybersecurity datasets without the need for manual feature engineering involved in conventional techniques. The findings are of profound implications for the field of cybersecurity because they offer a more automated, intelligent, and adaptive mechanism for detecting and mitigating threats in cloud environments. This will significantly affect real-time threat detection, anomaly recognition, and automated response mechanisms, thus making cloud infrastructures more robust and resilient. Despite all these strengths, further research has to be done to see how DB-IRF can be applied across different cloud infrastructures-that is, in hybrid, multi-cloud, and edge

computing-where security varies based on the architecture and deployment models. Furthermore, the integration of DB-IRF with other security technologies, such as blockchain for immutable logging, federated learning for distributed threat intelligence, or zero-trust architectures, can make it even more effective. Future studies could also investigate the real-time deployment of DB-IRF in active cloud environments, assessing its performance in live cybersecurity scenarios and optimizing its efficiency for large-scale threat detection. As cloud ecosystems continue to evolve, innovative frameworks such as DB-IRF will be fundamental in assuring proactive, intelligent, and adaptive security strategies that will neutralize sophisticated cyber threats.

List of Abbreviations

Abbreviation	Definition
CTI	Cyber Threat Information
SE	Selective Encryption
DWT	Discrete Wavelet Transform
EOS	Enterprise Operation System
OTP	One-Time Passwords
PIPA	Personal Information Protection Act
QKD	Quantum Key Distribution
KNN	k Nearest Neighbors
GNB	Gaussian Naïve Bayes
SVM	Support Vector Machines

Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this paper.

Funding

The authors receive no funding for this work.

Acknowledgment

None.

References

[1] Mughaid, I. Obeidat, L. Abualigah, S. Alzubi, M. S. Daoud, and H. Migdady, “Intelligent cybersecurity approach for data protection in cloud computing based internet of things,” *Int. J. Inf. Secur.*, pp. 1–15, 2024, doi: 10.1007/s10207-024-00832-0.

[2] S. Qi, Y. Lu, W. Wei, and X. Chen, “Efficient data access control with fine-grained data protection in cloud-assisted IIoT,” *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2886–2899, 2020, doi: 10.1109/JIOT.2020.3020979.

[3] S. Yalamati, “Data Privacy, Compliance, and Security in Cloud Computing for Finance,” in *Practical Applications of Data Processing, Algorithms, and Modeling*, IGI Global, 2024, pp. 127–144, doi: 10.4018/979-8-3693-2909-2.ch010.

[4] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, “Security and privacy-preserving challenges of e-health solutions in cloud computing,” *IEEE Access*, vol. 7, pp. 74361–74382, 2019, doi: 10.1109/ACCESS.2019.2919982.

[5] L. Ogiela and M. R. Ogiela, “Cognitive security paradigm for cloud computing applications,” *Concurrency Computat.: Pract. Exper.*, vol. 32, no. 8, p. e5316, 2020, doi: 10.1002/cpe.5316.

[6] Z. He, T. Zhang, and R. B. Lee, “Attacking and protecting data privacy in edge–cloud collaborative inference systems,” *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9706–9716, 2020, doi: 10.1109/JIOT.2020.3022358.

[7] S. Vinoth, H. L. Vemula, B. Haralayya, P. Mamgain, M. F. Hasan, and M. Naved, “Application of cloud computing in banking and e-commerce and related security threats,” *Mater. Today Proc.*, vol. 51, pp. 2172–2175, 2022, doi: 10.1016/j.matpr.2021.11.121.

[8] S. Shakya, “An efficient security framework for data migration in a cloud computing environment,” *J. Artif. Intell.*, vol. 1, no. 01, pp. 45–53, 2019, doi: 10.36548/jaicn.2019.1.006.

[9] D. W. Chadwick *et al.*, “A cloud-edge based data security architecture for sharing and analysing cyber threat information,” *Future Gener. Comput. Syst.*, vol. 102, pp. 710–722, 2020, doi: 10.1016/j.future.2019.06.026.

[10] H. Qiu, H. Noura, M. Qiu, Z. Ming, and G. Memmi, "A user-centric data protection method for cloud storage based on invertible DWT," *IEEE Trans. Cloud Comput.*, vol. 9, no. 4, pp. 1293–1304, 2019, doi: 10.1109/TCC.2019.2911679.

[11] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Future Gener. Comput. Syst.*, vol. 102, pp. 902–911, 2020, doi: 10.1016/j.future.2019.09.028.

[12] C. Yang *et al.*, "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70604–70615, 2020, doi: 10.1109/ACCESS.2020.2985762.

[13] A. M. Sauber *et al.*, "A new secure model for data protection over cloud computing," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–11, 2021, doi: 10.1155/2021/8113253.

[14] J. C. Liu, C. H. Lin, and K. Y. Lee, "Cloud-based personal data protection system and its performance evaluation," *J. Internet Technol.*, vol. 20, no. 6, pp. 1721–1727, 2019.

[15] S. J. N. Kumar, S. Ravimaran, and M. M. Alam, "An effective non-commutative encryption approach with optimized genetic algorithm for ensuring data protection in cloud computing," *Comput. Model. Eng. Sci.*, vol. 125, no. 2, pp. 671–697, 2020, doi: 10.32604/cmes.2020.09361.

[16] "KDD99 Dataset," *Kaggle*, [Online]. Available: https://www.kaggle.com/datasets/toobajamal/kdd99-dataset/data.

[17] X. Ma and X. Cheng, "Detection and analysis of network intrusion data set based on KNN algorithm," *World Sci. Res. J.*, vol. 7, no. 6, pp. 118–123, 2021, doi: 10.6911/WSRJ.202106_7(6).0015.

[18] N. Karmous, M. O. E. Aoueileyine, M. Abdelkader, and N. Youssef, "IoT real-time attacks classification framework using machine learning," in *Proc. 2022 IEEE 9th Int. Conf. Commun. Netw. (ComNet)*, 2022, pp. 1–5, doi: 10.1109/ComNet55492.2022.9998441.

[19] R. Kaushik, V. Singh, and R. Kumar, "Multiclass SVM based network intrusion detection with attribute selection using infinite feature selection technique," *J. Discrete Math. Sci. Cryptogr.*, vol. 24, no. 8, pp. 2137–2153, 2021, doi: 10.1080/09720529.2021.2009189.

[20] S. F. Jabbar, N. S. Mohsin, B. Al-Attar, and I. I. Al-Barazanchi, "Proposed framework for semantic segmentation of aerial hyperspectral images using deep learning and SVM approach," *Fusion: Pract. Appl.*, vol. 14, no. 2, 2024.

[21] S. F. Jabbar, N. S. Mohsin, J. F. Tawfeq, P. S. JosephNg, and A. L. Khalaf, "A novel data offloading scheme for QoS optimization in 5G based internet of medical things," *Bull. Electr. Eng. Inform.*, vol. 12, no. 5, pp. 3124–3133, 2023.

[22] S. Q. Salih, A. L. Khalaf, N. S. Mohsin, and S. F. Jabbar, "An optimized deep learning model for optical character recognition applications," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 3, pp. 3010–3018, 2023.

[23] A. M. Taha, S. F. Jabbar, and A. H. Alwan, "Sentiment retrieval of health records using NLP-based algorithm," unpublished.

[24] S. F. Jabbar, "Automated stand-alone surgical safety evaluation for laparoscopic cholecystectomy (LC) using convolutional neural network and constrained local models (CNN-CLM)," *J. Robot. Control*, vol. 3, no. 6, pp. 817–826, 2022.

[25] D. H. Rasheed, "Advancing energy efficiency with smart grids and IoT-based solutions for a sustainable future," *ESTIDAMAA*, pp. 37–43, 2024.

[26] I. Ibraheem, A. Barazanchi, and D. H. Rasheed, "The role of the Iraqi national data center in advancing digital transformation and data sovereignty," *SHIFRA*, vol. 2024, pp. 88–96, 2024.

[27] I. Ibraheem, A. Barazanchi, and D. H. Rasheed, "The role of green technologies in mitigating carbon footprints in industrial sectors," *ESTIDAMAA*, vol. 2024, pp. 31–36, 2024.

[28] F. S. Al-Mukhtar, Z. A. Jaaz, and A. H. Hamad, "Reliable fuzzy-based multi-path routing protocol based on whale optimization algorithm to improve QoS in 5G networks for IoMT applications," *Int. J. Interact. Mobile Technol.*, vol. 17, no. 6, 2023.