Semiconductor Optoelectronics
ISSN: 1001-5868

OPTIMIZING ENCRYPTION ALGORITHMS THROUGH BLOCKCHAIN SECURITY MACHINE LEARNING ALGORITHMS

Monika
Research Scholar, CSE Department, BMU, Rohtak, Haryana

Brij Mohan
Professor, CSE Department, BMU, Rohtak, Haryana

Vinit Kumar
Assistant Professor, CSE Department, VCE, Rohtak, Haryana

Abstract:
In the contemporary technological landscape, cloud computing and machine learning stand out as pervasive and influential technologies. However, the burgeoning use of cloud services raises concerns about data security, with unauthorized access posing a constant threat to crucial information. With the emergence of machine learning, supervised and unsupervised learning approaches have gained popularity in constructing robust security frameworks for cloud environments. This research focuses on leveraging machine learning algorithms to address data security challenges, with a specific emphasis on data confidentiality and integrity. To enhance the efficiency of data encryption processes, five supervised machine learning algorithms—Logistic Regression, Decision Tree, Random Forests, Extra Trees, and KNN—are compared in terms of their ability to classify data into critical and non-critical categories. The goal is to selectively encrypt only the critical data, thereby reducing computational complexity and improving overall data security.

Keywords: Logistic Regression, Decision Tree, Random Forests, Extra Trees, KNN, AES

1. INTRODUCTION

As the utilization of cloud resources has been exceptionally augmenting there is a substantial call for data security. Bulk amounts of data is being stored in the cloud and transmitted from/to the cloud. It is the significant duty of the cloud providers and cloud developers to deploy secure algorithms on the cloud data. Before understanding the security mechanisms that are to be provided to the cloud, it is the foremost duty of the developer to understand the types of cloud data and the policies that are to be followed to provide and

enhance the security of the data. Any security policy that is deployed on the cloud focuses on three security aspects. They are data integrity, data confidentiality and authentication. Cloud computing renders comprehensive resources like computational platforms, storage applications and computational power to the users. The data of all the users that is being aggregated in the cloud is escalating proportionately with the number of organizations that utilize resources in the cloud. Some of the substantial confronts that are being faced by cloud computing are security to the data and retrieving it over the network safely and rapidly.

In the context of classifying data into critical and non-critical categories for selective encryption, Extra Trees and K-Nearest Neighbors (KNN) are two machine learning algorithms that are employed to assess the significance of data points. Extra Trees, a type of ensemble learning method, is known for its high efficiency and ability to handle diverse datasets by constructing multiple decision trees and combining

their outputs. This makes it particularly suitable for large-scale data classification tasks. On the other hand, KNN relies on proximity-based analysis, assigning labels to data points based on the majority class among their nearest neighbors. The choice between these algorithms depends on the characteristics of the data and the specific requirements of the classification task. In the context of selectively encrypting critical data, the comparative analysis involves evaluating the algorithms' accuracy, computational efficiency, and adaptability to the targeted encryption strategy. The goal is to identify the algorithm that not only accurately distinguishes critical and non-critical data but also minimizes computational complexity, thereby enhancing overall data security by efficiently encrypting only the most vital information.

The major threats to data security are Data confidentiality, Data integrity and Authentication to the data and user. Lots of research is being carried out to enhance the cloud security and also various middleware tools, security frameworks are being built. As is the increase in security infrastructure, there is proportionate increase in the new form of attacks and intrusions. In order to encounter such attacks there is dire need for the researchers to embed innovative security algorithms [4]. To enhance the existing security infrastructures, they are being steered and powered by machine learning algorithms. Explicit programming will not be a pre requisite when machine learning algorithms are used for cloud data security. All they do is learning and analyzing from the data relying on historic data. As there are major advancements in machine learning, ML algorithms can classify the entities as authorized or unauthorized and data as trivial or non-trivial.

Machine learning algorithms play a vital role in providing cloud security. They are used to detect the intruders by which prevention of unauthorized access can be performed. It also can be checked on the network whether the data that is being transmitted is in encrypted format or not. Supervised ML algorithms can be used to detect any malicious activity if performed on the cloud data [5]. They are deployed with the cloud servers to analyze the traffic load and the resources performances. In cloud computing one of the major challenging issues is data loss. This can be conquered using dynamic data masking method which is developed using machine learning. By using the important feature of ML i.e. Prediction, it can be depicted whether cloud is functioning normally/abnormally. From the above perception of various studies, it is assumed that machine learning algorithms can be major contributors in enhancing cloud security [5]. The number of traffic accidents and their casualties appears to be increasing internationally due to increased motorization and population [6]. Complicated traffic circumstances and unexpected incidents endanger the safety of drivers, passengers, and pedestrians. Traffic accidents have become a key issue for transportation security as populations and car numbers have grown. Accidents on the road raise insurance, medical, and monetary expenditures. Diverse components in traffic accidents have a substantial impact on one another, making it difficult to take any of the criteria independently when describing the severity of traffic accidents. The development of effective methods for predicting and grading crash injury severity, which rely on various explanatory variables, was a crucial aspect in traffic safety research [7]. Accident management mechanisms play an important role in emergency systems and traffic control. Data from various sources is gathered in such structures for the purpose of assisting injured persons [8].

Photographs and measurements obtained at the scene of an accident are the most important pieces of evidence in accident lawsuits. Police or investigators alter data gathered at the scene of an accident. If police and investigators know exactly what they will use the images they take

at the site for, there should be no space for error in accident investigations. Rather than taking a dozen random photographs, it is more effective to plan out a succession of high-quality images. Access to high-quality photos of the accidents is critical for accident analysis.

Image source is a critical data source in accidents. Such photos can be captured by either portable or fixed cameras, but the latter is far more effective. Such digital photos typically contain a plethora of personally sensitive data. When attackers analyse and acquire data, unquantifiable losses occur, as does

the exposure of personal privacy [9]. Image privacy is routinely protected using methods such as privacy encryption, k-anonymity, and access restriction. According to the visual data-protection system, several perceptual encrypted strategies were modelled to make images without visual data, whereas data theory-related encryption (AES and RSA) generates cipher text [10]. Perceptual encryption aims to generate images without visual data on simple images using a visual data-protection method since visual data contains private information such as personally identifying information, time, and location [11].

For object categorization, [12] recommend a hybrid PPDL technique. This research tries to improve satellite image encryption while maintaining object classifier accuracy and runtime. The public keys of relatively homomorphic encryption and Paillier homomorphic encryption are used to protect the picture encryption approach. Chuman and Kiya [13] created a learnable picture encryption approach for privacy-preserving deep neural networks. The presented solution employs block scrambling in conjunction with data augmentation methods such as grid mask, random cropping, and horizontal flip. The use of block scrambling enhances robustness against numerous attacks; nevertheless, when combined with data augmentation, it allows for the preservation of higher classifier accuracy while employing encrypted images. He et al. [14] created Crypto Eyes to address the issues with privacy-preserving classifiers on encrypted images. The article provides a 2-stream convolution network structure for the classifier of encrypted images to capture the contour of the encrypted image, significantly enhancing classification accuracy. Shen et al. [15] created a safe SVM, which is a privacy-preserving SVM training system that runs on blockchain (BC)-based encrypted IoT data. The author employs the BC technique to build dependable and secure data sharing platforms for multiple data providers, while IoT data is encrypted and recorded on the distributed ledger. Ito et al. [16] created a transformation technique for visually protected images in privacy- preserving DNN. However, the presented technique allows us to maintain image classification performance while also protecting visual information.

The authors of [17] address the issues by developing Secure DL, a privacy-preserving image detection algorithm for encrypted datasets stored in the cloud. The provided block-based picture encryption solution is well-developed for the protection of visual data in images. The provided technique is shown to be secure from a probabilistic standpoint and against various cryptographic attacks. Ahmad and Shin [18] describe a powerful pixel-based encryption method. The technology provides a minimal amount of privacy while preserving the inherent property of the source images, allowing DL application in the field of encryption. For the lower calculation need, the author used logistic maps. Furthermore, to compensate for any inefficiency caused by the logistic maps, the author employs a second key to shuffle the sequence.

On the other hand, there are some authors who specialise in analysing accidents. Several image-processing algorithms were developed in order to develop a real-time mechanism to aid the accident [20]. Crash severity algorithms can predict the severity of a crash, allowing clinics to provide correct health care as soon as feasible [21]. Furthermore, study on crash injury severity contributes to a better understanding of what factors contributed to injury severity after a crash, which will help enhance road safety and reduce crash severity. Crash severity was traditionally defined by a variety of separate types of possible injury, including lethal, incapacitating, property damage only, and non-incapacitating [22].

Deep-learning (DL) models have achieved remarkable performance in a variety of disciplines, including autonomous driving systems, as processing power and technology have improved. Now that neural networks (NN) have grown into a powerful tool for detecting intricate patterns in high-dimensional datasets and making correct predictions, they can be trusted to generate accurate and reliable projections in ordinal data. Some of these strategies use machine learning (ML) techniques like artificial neural networks (ANN). Hidden characteristics can be extracted using pooling layers [23]. In general, the

output of the final pooling layer was used for regression and classification.

The most crucial evidence is photographs and measurements taken at the scene of the accident. Attackers will steal data and violate people's privacy, causing enormous damage. Image encryption can be used to achieve cloud storage [24] and secure image transmission in the network; additionally, an automated deep-learning (DL)-based accident severity classification is required.

2. PROPOSED METHOD

Generally, the cloud data is classified as Public, Private and Confidential and all the data that resides in the cloud has certain metrics. Data encryption is performed to provide Data confidentiality which is one of the significant security metrics. Suppose if we have to encrypt the entire data set it may take much time rather than encrypting only the fields that are to be hidden. In order to classify the fields of data sets as readable and hidden, we have used machine learning algorithms. Whenever a data set with huge set of records has to be stored in the cloud, as the foremost step the data sets are to be classified. Later the class of data which was classified from the given data set should be encrypted. The architecture of the proposed method is described in the below figure 1.

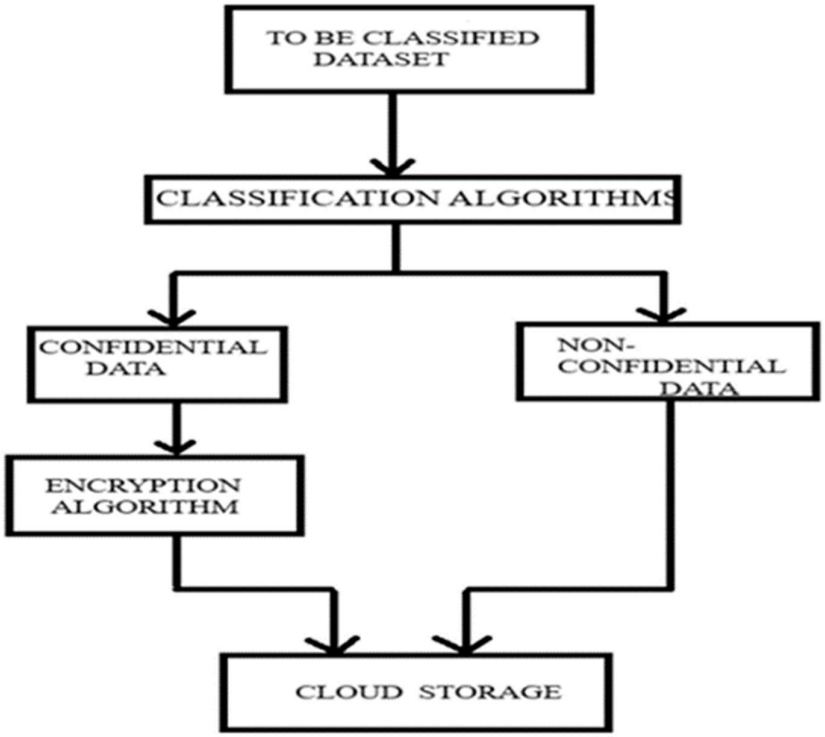

Fig.1.Proposed Mechanism

2.1 DATA CLASSIFICATION

Machine learning algorithms are being used to classify the data in wide variety of domains in recent years. In our proposed method we have classified the data using five supervised learning algorithms. They are Logistic Regression, Decision Tree, Random Forests, Extra Trees and KNN that are used for data classification. These are the algorithms which were proved to be the best in terms of performance for classification. We have implemented all the algorithms on the chosen data sets to check which one outperforms the other. The need of data classification is to reduce the computational time taken by the

encryption algorithms [1]. Data classification is the process of sorting data into classes depending on its attribute value and the level of security it needs. It aids us to prioritize the efforts that we have to put to secure the cloud data and also regularity compliance. The classification algorithms that were implemented are discussed in the below sections.

2.1.1 LOGISTIC REGRESSION

For binary classification assignments where the target variable has two classes, logistic regression is typically utilized. By fitting a logistic function to the inputs, it calculates the chance that an event falls into a particular class. To determine the parameters that optimize the likelihood of the observed data, optimization techniques are used. The Logistic function is a non-linear, sigmoid function with an S-shaped curve. It is perfectly bounded between 0 and 1, which is what probabilities need. They may be sensitive to data noise and outliers [7].

2.1.2 DECISION TREE

A decision tree is a structure similar to a flowchart, in which each leaf node denotes a result, each branch denotes a decision rule, and each interior node denotes a function. It divides the data recursively into homogenous subsets with regard to the target variable using function values as the basis. It is responsible and capable of handling both classification and regression jobs. Even on enormous datasets, decision trees can be trained reasonably quickly. The problem with over fitting is that decision trees may learn the training set of data too thoroughly and fail to generalize to the set of new data. Cross-validation and pruning approaches can be used to reduce this.

2.1.3 RANDOM FORESTS

A forecast is made using an ensemble technique called random forests, which combines different decision trees. With the use of various subsets of the training data and arbitrary feature selections, it produces a number of decision trees. It employs a method known as bagging i.e bootstrap aggregation which entails the creation of several bootstrap samples of training data and the subsequent training of a decision tree on each sample. This makes the ensemble more resilient by lowering the variance of the individual trees. In order to arrive at the final forecast, the predictions from each individual tree are added together, or in the case of voting or regression, average, or voting in the case of classification. This lessens over fitting and increases generalizability.

2.1.4 EXTRA TREES

Similar to Extremely Random Trees, Random Forests combine a group of decision trees to improve prediction performance; however, they take a different technique to adding unpredictability [6]. Extremely Random Trees add an additional layer of randomization by using arbitrary thresholds for splits, increasing tree diversity, whereas Random Forests use the best thresholds for partitioning. In addition to cultivating a wider variety of trees within the ensemble, this intentional randomization also has the potential to improve overall model efficacy by lowering over fitting and boosting resilience. This approach demonstrates how controlled chaos can be used to increase an ensemble learning technique's overall predictive capability, making it a compelling choice in the field of machine learning.

2.1.5 K-NEAREST NEIGHBORS (KNN)

K-Nearest Neighbors (KNN) is an example of how machine learning may be elegantly simple while still being extremely effective at both classification and regression tasks. Based on the proximity principle, KNN assigns a novel data point to a certain class or predicts regression by determining the consensus or mean of its attributes from the nearby k data points in the feature space. Making an acceptable choice for K, which directly determines how much surrounding data points influence the

final prediction, is the key decision. A bigger K enables a smoother prediction contour, encompassing more global patterns, whereas a smaller K tends to produce a more sensitive model, prone to catching local details. Such flexibility in responsiveness facilitates KNN's use for various applications, though the practitioner must carefully calibrate K to take advantage of its true potential.

2.2 ENCRYPTION METHOD

The proposed system incorporates classification algorithms to distinguish attributes requiring security measures from those that do not. Only the attributes along with their values that are considered to necessitate security are selected as inputs for the encryption algorithm. The implementation employs AES, a symmetric encryption algorithm, for the purpose of data encryption. The utilization of a symmetric algorithm enables the provision of both data confidentiality and authentication. Following encryption, the data is categorized into two classes, wherein one class is maintained in an encrypted format while the other remains unaltered. This sequential process significantly contributes to a reduction in encryption time. AES algorithm is applied to both the entire dataset and the classified subset. Notably, the time complexity is observed to have decreased by over fifty percent (50%).

3. Results and Analysis

Logistic Regression is a statistical model used for binary classification tasks, where the goal is to predict one of two possible outcomes based on input features. It's called "logistic" because it employs the logistic function to model the relationship between the input variables and the probability of a specific outcome. Unlike linear regression, which predicts continuous numeric values, logistic regression estimates the probability that an input belongs to one of the two classes, typically represented as 0 or 1. It accomplishes this by transforming a linear combination of input features into a probability score between 0 and 1, making it a valuable tool in various fields, such as medicine, finance, and machine learning, for tasks like spam detection, disease diagnosis, and credit risk assessment.

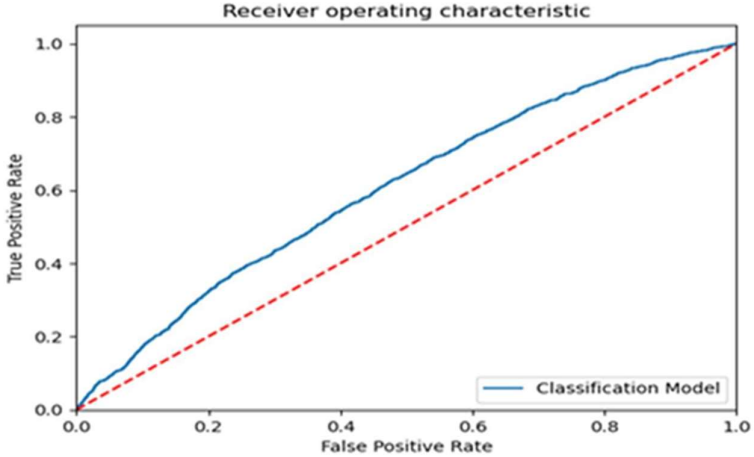

Fig.2.Analysis of Logistic Regression

The Decision Tree Classifier is a machine learning algorithm used for both classification and regression tasks. It is a part of the Decision Tree family of algorithms, which are based on a tree-like structure where nodes represent decisions or choices, branches represent possible outcomes, and leaves represent the final predictions or class labels. In classification tasks, the Decision Tree Classifier builds a tree by recursively splitting the dataset based on the features that provide the best separation between classes. It aims to create branches that result in pure or nearly pure class labels at the leaves. When making predictions, the algorithm traverses the tree from the root node to a leaf node based on the input features, and the class label associated with that leaf node becomes the prediction.

Decision trees have the advantage of being interpretable and easy to visualize, making them valuable for understanding the decision-making process in a model. However, they can be prone to overfitting,

especially when the trees are deep and capture noise in the training data.

Techniques like pruning and setting maximum depth can help mitigate overfitting. Overall, the Decision Tree Classifier is a versatile algorithm widely used in machine learning for tasks like classification, and it serves as the foundation for more complex ensemble methods like Random Forests and Gradient Boosting.

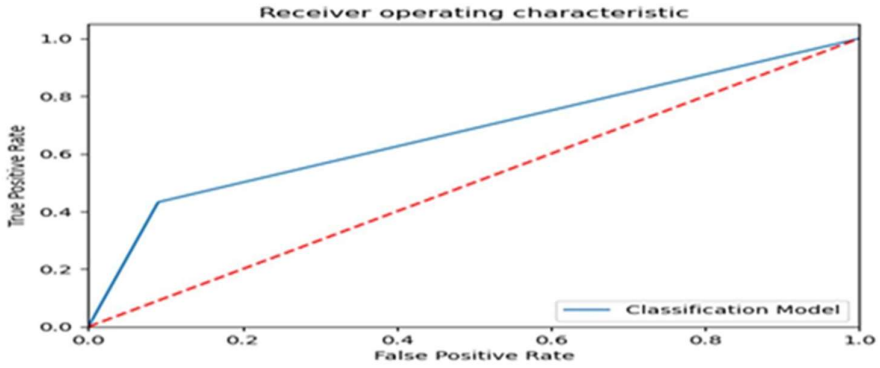

Fig.3. Analysis of Decision Tree Classifier

The Random Forest Classifier is a versatile and highly regarded machine learning algorithm, primarily employed for classification tasks within the realm of supervised learning. Its fundamental principle involves constructing an ensemble of decision trees to collectively make accurate predictions. This ensemble approach provides several advantages over single decision trees. At its core, the algorithm begins by generating multiple decision trees. To introduce diversity and reduce bias, each tree is trained on a random subset of the original dataset. This process, known as bootstrapping, involves selecting data points with replacement. Furthermore, to ensure that the individual trees possess distinctive characteristics, a random subset of features is chosen for each tree. This step is crucial for preventing trees from always selecting the same features, which could lead to correlation among them.

Each of these decision trees operates independently, using its designated subset of data and features to make predictions. When presented with a new data point, every tree casts its vote for the class label it deems most appropriate. The final classification decision is then determined through a process of majority voting. In the case of a binary classification problem, the class that receives the majority of votes becomes the predicted class label. This democratic approach to decision-making contributes to the algorithm's robustness and ability to provide accurate predictions. Random forests have garnered widespread acclaim for their exceptional performance in a multitude of classification tasks. They are particularly well-suited for scenarios involving high-dimensional data, where many features must be considered simultaneously. Additionally, their built-in mechanism for feature selection and their ability to handle noisy datasets make them an excellent choice for practical applications. Furthermore, random forests are known for their innate resistance to overfitting, which means they can generalize effectively to new, unseen data.

Due to these remarkable attributes, random forests have found applications in a wide spectrum of domains, including image recognition, where they excel in classifying objects within images, spam detection, where they effectively discern between legitimate and spam emails, and medical diagnosis, where they assist in identifying diseases or conditions based on patient data. In summary, the Random Forest Classifier is a powerful tool in the arsenal of machine learning algorithms, celebrated for its accuracy, robustness, and adaptability across various classification challenges.

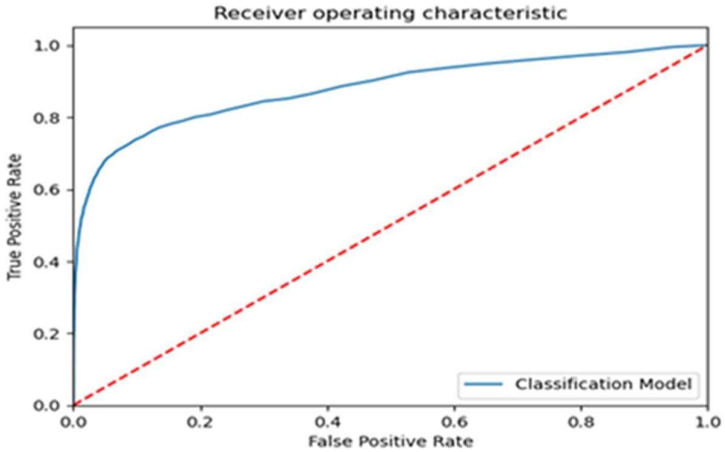

Fig.4. Analysis of Random Forest Classifier

Gaussian Naive Bayes (Gaussian NB) is a classification algorithm that relies on the principles of probability theory to make predictions, particularly suitable for datasets with continuous or real-valued features following a Gaussian distribution. During training, it estimates the Gaussian distributions (mean and variance) for each feature within each class, assuming feature independence. In the prediction phase, Gaussian NB calculates the likelihood that a new data point belongs to each class, using Bayes' theorem, and assigns it to the class with the highest posterior probability. Despite its simplicity and the "naive" assumption of feature independence, Gaussian NB is widely used in applications like text classification, spam detection, and medical diagnosis, where it often delivers accurate results with computational efficiency.

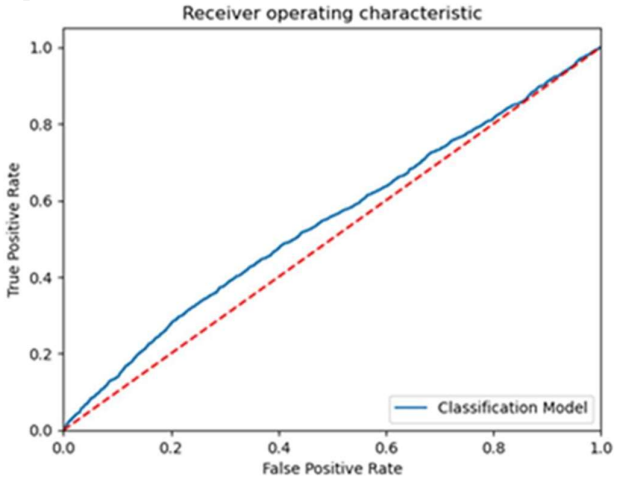

Fig.5. Analysis of Gaussian NB

The KNeighbors Classifier is a supervised machine learning algorithm used for both classification and regression tasks. It operates on the principle of proximity, where it classifies a new data point by examining the class labels of its k-nearest neighbors in the training dataset.

The algorithm calculates distances, typically Euclidean, between the new data point and all the training data points to identify the k-nearest neighbors. In classification, it assigns the class label that occurs most frequently among the neighbors, while in regression, it computes the average of the target values of the neighbors. KNeighbors Classifier is a versatile and intuitive algorithm, suitable for various applications, including image recognition, recommendation systems, and anomaly detection, but the choice of the appropriate value of 'k' is crucial for its performance.

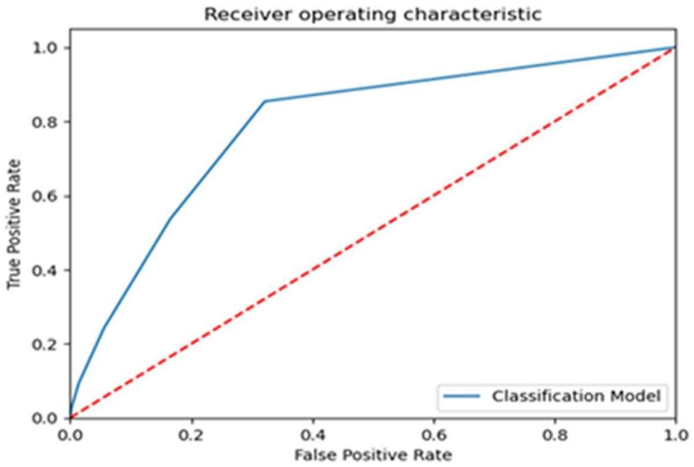

Fig.6. Analysis of KNeighbors Classifier

The Extra Trees Classifier, an ensemble machine learning algorithm, akin to Random Forests, specializes in classification tasks but can also be adapted for regression. It builds a collection of decision trees, but with a distinctive twist – it introduces additional randomness by randomly selecting features for splitting at each node during tree construction, which is known as being "extremely randomized." This randomization reduces the risk of overfitting and enhances diversity among individual trees. The algorithm's benefits include reduced overfitting, efficient parallelism for large datasets, feature importance analysis, and robustness to hyper parameter settings. Extra Trees Classifier finds applications in various fields, such as image classification, anomaly detection, and fraud detection, thanks to its capability to handle complex, high- dimensional data while improving predictive performance.The Extra Trees Classifier stands out as a robust machine learning algorithm with several advantages, notably its capacity to mitigate overfitting and enhance diversity among individual trees through the implementation of randomization techniques. This not only promotes more accurate generalization to unseen data but also facilitates efficient parallel processing, making it well-suited for handling large datasets. Moreover, the algorithm offers the advantage of feature importance analysis, allowing users to gain insights into the significance of different features in the classification process. With its versatility, the Extra Trees Classifier has found applications across diverse fields, including image classification, anomaly detection, and fraud detection. Its ability to effectively manage complex, high-dimensional data contributes to improved predictive performance, making it a valuable tool in various real-world scenarios.

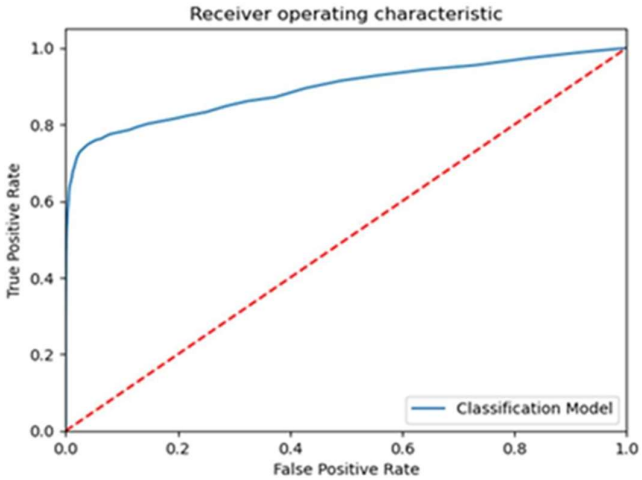

Fig.7. Analysis of Extra Trees Classifier

In Table 1 we have depicted the outcomes of classification using various algorithms including Logistic

Regression, Decision Tree, Random Forests, Extra Trees, and KNN. The results demonstrate that Extra Trees exhibit a notably higher accuracy percentage compared to the other deployed algorithms.

Table.1. Classification of Data

Prior Classification		After Classification				Accuracy (%)				
		Class 1		Class 2		Logistic Regression	Decision Tree	Random Forests	Extra Trees	KNN
Size of File	No of Attributes	Size of File	No of Attributes	Size of File	No of Attributes	87	84.7	91.3	93.6	85.3
6247(KB)	26	2400(KB)	10	3847 (KB)	16					

After data classification, data that has to be secured is passed to the encryption algorithm. In our proposed method, initially we have encrypted the data using AES algorithm with block and key size of 128 bits. Later we have encrypted data of Class 1 to calculate the difference in their executions. The execution time is remarkably reduced by more than half. Table 2 represents the comparison table of AES for the entire data and classified data.

Table.2. Performance Comparison table of AES

Data Size (KB)	Encryption Speed (MB/Sec)	Encryption Time (ms)	Encryption Time (ns)
6247	100	62.47	62,470
2400	80	30	30,000

4. CONCLUSION

In this study, we have employed a range of classification algorithms from the realm of machine learning to effectively categorize data into two classes: confidential and non-confidential. Our analysis encompassed the implementation of five distinct classification algorithms; each meticulously evaluated for its performance characteristics. Extra Trees classifier is chosen as the optimal choice for accurate data classification. In the context of data security, classification algorithm has isolated parameters that need protection which were passed to encryption algorithm. Subsequently, this encrypted data was securely stored within the cloud environment. Conversely, data falling into the non-confidential category was stored within the cloud without undergoing encryption. This research underscores the significance of methodical algorithm selection for data classification, with Extra Trees exhibiting notable proficiency. Moreover, our approach to data partitioning and encryption aligns with the broader objective of data security, catering to the specific needs of sensitive information while maintaining efficiency in storage. Through the fusion of machine learning and data security paradigms, this study contributes to the advancement of robust and tailored data management practices.

REFERENCES

1. M. A. Zardari, L. T. Jung and N. Zacharias, "K-NN classifier for data confidentiality in cloud computing," 2014 International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 2014, pp. 1-6.
2. DSharma, S., Rama Krishna, C., Sahay, S.K. (2019). Detection of Advanced Malware by Machine Learning Techniques. In: Ray, K., Sharma, T., Rawat, S., Saini, R., Bandyopadhyay, A. (eds) Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing, vol 742. Springer, Singapore.
3. D. Bhamare, T. Salman, M. Samaka, A. Erbad and R. Jain, "Feasibility of Supervised Machine Learning for Cloud Security," 2016 International Conference on Information Science and Security (ICISS), Pattaya, Thailand, 2016, pp. 1-5.
4. Purushothaman and S. Abburu, "An Approach for Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, vol. 9, no. 2, March 2012.
5. Z. Masetic, K. Hajdarevic and N. Dogru, "Cloud computing threats classification model based on the detection feasibility of machine learning algorithms," 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2017, pp. 1314-1318.
6. A. K. V, A. A, B. Jose, K. Anil Kumar and O. T. Lee, "Phishing Detection using Extra Trees Classifier," 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-6.
7. J. R. Brzezinski and G. J. Knafl, "Logistic regression modeling for context-based classification," Proceedings. Tenth International Workshop on Database and Expert Systems Applications. DEXA 99, Florence, Italy, 1999, pp. 755-759.
8. Alkhelaiwi, M.; Boulila, W.; Ahmad, J.; Koubaa, A.; Driss, M. An efficient approach based on privacy-preserving deep learning for satellite image classification. Remote Sens. 2021, 13, 2221. Rehman, M.U.; Shafique, A.; Ghadi, Y.Y.; Boulila, W.; Jan, S.U.; Gadekallu, T.R.; Driss, M.; Ahmad, J. A Novel Chaos-Based Privacy-Preserving Deep Learning Model for Cancer Diagnosis. IEEE Trans. Netw. Sci. Eng. 2022, 9, 4322–4337.
9. Nakamura, K.; Nitta, N.; Babaguchi, N. Encryption-free framework of privacy- preserving image recognition for photo-based information services. IEEE Trans. Inf. Secur. 2018, 14, 1264–1279. [Ito, H.; Kinoshita, Y.; Aprilpyone, M.; Kiya, H. Image to perturbation: An image transformation network for generating visually protected images for privacy- preserving deep neural networks. IEEE Access 2021, 9, 64629–64638.
10. Popescu, A.B.; Taca, I.A.; Vizitiu, A.; Nita, C.I.; Suciu, C.; Itu, L.M.; Scafa-Udriste,
A. Obfuscation Algorithm for Privacy-Preserving Deep Learning-Based Medical Image Analysis. Appl. Sci. 2022, 12, 3997.
11. Kaissis, G.; Ziller, A.; Passerat-Palmbach, J.; Ryffel, T.; Usynin, D.; Trask, A.; Lima, I.; Mancuso, J.; Jungmann, F.; Steinborn, M.M.; et al. End-to-end privacy preserving deep learning on multi-institutional medical imaging. Nat. Mach. Intell. 2021, 3, 473–484.
12. Huang, Q.X.; Yap, W.L.; Chiu, M.Y.; Sun, H.M. Privacy-Preserving Deep Learning with Learnable Image Encryption on Medical Images. IEEE Access 2022, 10, 66345–66355.
13. Abdullah, S.M. Survey: Privacy-Preserving in Deep Learning based on Homomorphic Encryption. J. Basrah Res. (Sci.) 2022, 48.
14. Boulila, W.; Ammar, A.; Benjdira, B.; Koubaa, A. Securing the Classification of COVID-19 in Chest X-ray Images: A Privacy-Preserving Deep Learning Approach. arXiv 2022, arXiv:2203.07728.
15. El Saj, R.; Sedgh Gooya, E.; Alfalou, A.; Khalil, M. Privacy-preserving deep neural network methods: Computational and perceptual methods An overview. Electronics 2021, 10, 1367.
16. Praveen, S.P.; Sindhura, S.; Madhuri, A.; Karras, D.A. A Novel Effective Framework for

Medical Images Secure Storage Using Advanced Cipher Text Algorithm in Cloud Computing. In Proceedings of the 2021 IEEE International Conference on Imaging Systems and Techniques (IST), Kaohsiung, Taiwan, 24–26 August 2021; pp. 1–4.
17. Boulila, W.; Khlifi, M.K.; Ammar, A.; Koubaa, A.; Benjdira, B.; Farah, I.R. A Hybrid Privacy-Preserving Deep Learning Approach for Object Classification in Very High- Resolution Satellite Images. Remote Sens. 2022, 14, 4631.
18. Chuman, T.; Kiya, H. Block scrambling image encryption used in combination with data augmentation for privacy-preserving DNNs. In Proceedings of the 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), Penghu, Taiwan, 15– 17 September 2021; pp. 1–2
19. He, W.; Li, S.; Wang, W.; Wei, M.; Qiu, B. Crypto Eyes: Privacy Preserving Classification over Encrypted Images. In Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications, Vancouver, BC, Canada, 10–13 May 2021; pp. 1– 10.
20. Shen, M.; Tang, X.; Zhu, L.; Du, X.; Guizani, M. Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet Things J. 2019, 6, 7702–7712.
21. Ito, H.; Kinoshita, Y.; Kiya, H. Image transformation network for privacy-preserving deep neural networks and its security evaluation. In Proceedings of the 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE), Kobe, Japan, 13–16 October 2020; pp. 822– 825.
22. Tanwar, V.K.; Raman, B.; Rajput, A.S.; Bhargava, R. Secured: A privacy preserving deep learning model for image recognition over cloud. J. Vis. Commun. Image Represent. 2022, 86, 103503. Ahmad, I.; Shin, S. A Pixel-based Encryption Method for Privacy- Preserving Deep Learning Models. arXiv 2022, arXiv:2203.16780.