

Security of private cloud using machine learning and cryptography

Ali Abdulsattar Jabbar, Wesam Sameer Bhaya

Department of Networks Information, College of Information Technology, University of Babylon, Al-Hillah, Iraq

Article Info

Article history:

Received Jul 7, 2022

Revised Aug 30, 2022

Accepted Sep 19, 2022

Keywords:

Cloud security
Data classification
Cryptography
Machine learning

ABSTRACT

There are increased security challenges that target cloud systems. One of the most important requirements of users in cloud storage is protecting their cloud from attacks and keeping data secure. Modern technologies of machine learning are providing the ability to analyze and classify data perfectly. This paper proposes a model placed between users and the cloud, which is based on two phases. The first of which is protecting the cloud from different types of network attacks and detecting normal and abnormal flow. The second one is categorizing the users' data and then encrypting it based on its importance using different encryption algorithms. The accuracy results of random forest (RF) and decision tree (DT) are 100% of attack detection for each one. For the second phase of classifying data, the algorithms used are the logistic regression (LR) and stochastic gradient descent (SGD) learning which resulted in 98% accuracy for both. Besides, the encryption algorithms that have been adopted are rivest cipher (RC4), triple data encryption (3DES), and advanced encryption standard (AES) for encryption of the classified data according to the importance which will be then stored in the cloud in its secure form.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ali Abdulsattar Jabbar

Department of Networks Information, College of Information Technology, University of Babylon

51002, Babylon, Iraq

Email: ali.jabbar@student.uobabylon.edu.iq

1. INTRODUCTION

The private cloud is one of the most important services in computing, which allows the possibility of providing the service either in public via the internet, or in particular via an internal network, and users or clients choose private cloud services based on institutions and service companies with many benefits that provide them with public cloud services, as it provides them with self-service and expandable devices and flexibility in dealing with data in addition to many control and management advantages over various sources within the network infrastructure. Moreover, the private cloud network provides a very high level of security and privacy by relying on firewall services and internal hosting to ensure the reliability of operations and statements that are carried out only by authorized parties and do not allow unauthorized persons to access these services [1]. There are many related research directions presented in this work.

A threat classification scheme was proposed in [2] which is used to detect security issues threats, taking into consideration three various criteria: the first is the machine learning (ML) algorithm as supervised or unsupervised learning, the second is determining the input model features, and the third is based on the type of threats such as, the state of network-specific threats or cloud-specific threats. Research by He *et al.* [3] they suggest a detection system based on the denial of service (DoS) attack within the source side element in the cloud network, based on specific ML techniques. The used system gets benefits from the statistical

information efficiency of both components the cloud server's hypervisor and the virtual machines, and consequently to provide a control rule preventing particular network packages from being sent out to the outside network.

A data protection model was proposed in [4] as a suitable way to work within cloud computing, through an algorithm adopted to optimally deal with the data in private data of cloud computing, and represented by a public-key algorithm as rivest shamir adleman (RSA). Furthermore, a protocol was used, namely challenge handshake authentication protocol (CHAP), as authentication ciphertext challenge handshake which is represented by the protocol to improve the data authentication. It provides secure authentication for communicating parties within the network, as the results proved the proposed model safe and practical. According to Kolli *et al.* [5], a system was proposed for improving the data protection mechanism within the cloud network based on two factors, which is implemented depending on the cloud system, as the sender sends an encrypted message to the recipient using the cloud environment then the process of retrieving the encrypted message is done through two factors the first of which is a unique security device that is independent device connected to the computer system, while the second factor is a secret private key stored in the computer system. The results show the confidentiality of the cloud data together with revocability services.

Research by Mašetić *et al.* [6] an algorithm has been proposed based on the support vector machine (SVM) algorithm. The evaluation of results depends on several stages which based on categorizing DoS attacks and normal network behaviors. By the same token, these stages are represented by simulating the attack, collecting the data, choosing the features and classification, moreover the results prove the ability of the proposed system, depending on this algorithm, to detect DoS attack within the cloud computing environment.

The proposed method is based on a specific system that depends on the principle of an intrusion detection system (IDS) in [7]. The used system as a network intrusion detection system (NIDS) to detect anomaly-based cases, as it monitors, analyzes, and detects traffic of data targeting the cloud environment. The proposed system was based on dealing with types of attacks (DoS, Probe, R2L, U2R). In addition, the proposed system used a SVM to classify connections to a network. The results show the intrusive network connections detecting and high detection accuracy with low false alarm rates (FARs). Virupakshar *et al.* [8] relied on dealing with DDoS attacks, the proposed method targets the various types of networks, especially the cloud networks, which greatly affect them to stop the various services provided by this network in order for the entire network to be weak and disrupted as the proposed system implemented with OpenStack. Where the results indicated that the proposed system is a secure model that provides very integrated protection for monitoring data traffic, as algorithms were also used a specific scheme which eventually is DDoS attacks detecting also the administrator of the private cloud is notified based on decision tree (DT), K nearest neighbor (KNN), Naive Bayes, and deep neural network (DNN) algorithms for a training model to detect these types of attacks.

Tor Hammer attacking mechanism and IDS has been proposed in [9] and implemented in cloudstack environment to work with a novel dataset. The dataset analyzed with different ML algorithms as the k-means, DT, random forest (RF), Naïve Bayes, SVM, and C4.5. The result shows the best result for network performance analysis and accuracy with intrusion detection in the case of C4.5 and SVM algorithms [10]. It is clear that each of the reviewed works suffer from some limitations such as encoding within preprocessing, modeling stage issues with classifier choice, less use of multiple classifiers, and finally, outdated datasets are used in most of the studies. As a matter of fact, a security is considered a key requirement for the cloud as a meaningful solution. These risks have motivated us to think about a solution to protect data stored in private cloud and the proposed system provides a better solution to deal with these limitations sorted from related works.

ML is being increasingly utilized for a variety of applications of IDS and others. An IDS is a system that monitors and analyzes data to detect any intrusion in the system or network requests [11]. In other words, ML algorithms are used to solve security issues and manage data efficiently as a combination module with IDS to deal with the security issues in the cloud system, by training the system model to classify data traffic as normal and abnormal flow. In this paper, improving the secure private cloud using ML and cryptography is implemented. It is presented as follows: section 1 is introduction, section 2 is the proposed algorithm, section 3 is method, section 4 is results and discussion, and section 5 is conclusion.

2. THE PROPOSED CLOUD SECURITY ALGORITHM

To secure private cloud we have suggested the model work as third party between users and this private cloud. Figure 1 shows a general view of proposed work. The work being built based on ML techniques to work in two phases with two datasets. In the first phase, user requests are classified as normal or abnormal (malicious (attacks)). Next, normal requests are passed and the malicious ones are dropped. A datasets UNSW-NB15 is adopted to train the classifier in this stage, which is considerably recommended for configuring such systems; in the second stage of the model, users' (natural) requests are taken and their data

stored in the cloud is classified according to their importance (high confidentiality, confidentiality, basic). Finally, data is encrypted according to its last classification with algorithms.

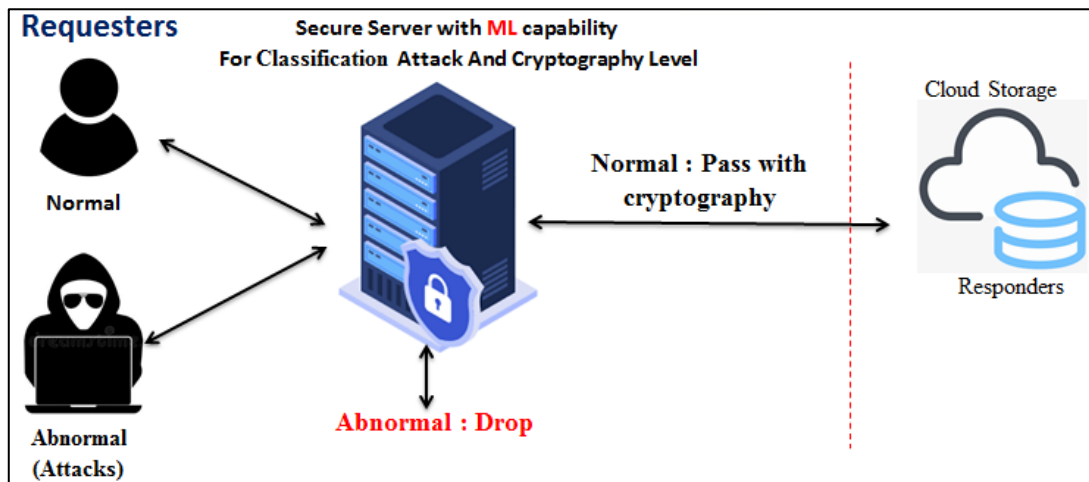


Figure 1. General view of the proposal

AES, 3DES and RC4 encryption algorithms are used. There was a challenge to find a data set with label classes in a degree of confidentiality, so the BBC News data set was chosen to train the classifier into their different classes including business, entertainment, politics, sport, and technology records. Figure 2 shows the proposed approach of unclassified request based on the two phases of request classification and data classification.

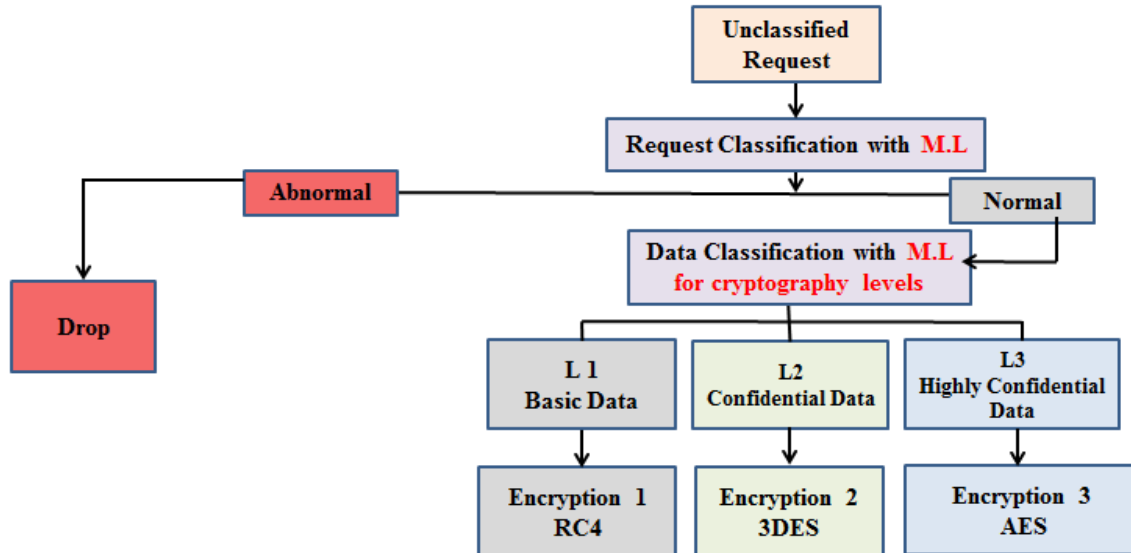


Figure 2. The proposed system approaches

2.1. Intrusion detection system

The first stage of the proposed system is based on the status of IDS. So, the proposed system detects the normal behavior from the malicious behavior of incoming requests to access the databases. The dataset UNSW-NB15 is one of the most important private datasets to deal with data analysis within the IDS state, a large set of raw data being captured to build this dataset. Likewise, various network analysis tools are represented as IXIA Perfect Storm tool and a TCPdump tool. In addition, it contains several properties created using Argus tool, the Bro-IDS tool, and 12 developed algorithms. Also, the number of properties is determined as 29 features which have been classified into five groups: flow features, basic features, content

features, time features, and additional generated features. Besides, this command includes the database counted types of attacks from them: backdoor, DoS, generic, reconnaissance, analysis, Fuzzers, Exploit, Shellcode, and Worms. The UNSW-NB15 dataset comes along with pre-defined splits of a training set of 175,341 samples and a testing set of 82,332 samples. However, the publicly available training and testing set both contain only 44 features: 42 attributes and 2 classes. Only the training set of UNSW NB15 training set is used for both training and testing in this paper. Actually, the primary focus is binary classification. The UNSW-NB15 Distribution sample was performed as a preprocessing on the data set using a specific method called integer encoding. The first step was integer encoding, thereupon each unique category value was assigned an integer value. For example, in the protocol type column, “TCP” is 1, “UDP” is 2, and “OSPF” is 3. This is known as a label encoding concept or an integer encoding. In some cases, it proved to be enough. The integer values have a natural ordered relationship between one another and ML algorithms may be able to understand and get benefits from such a relationship. Notably, ordinal variables in this case the “UDP” example above would be a good example as a label encoding would be sufficient. Equally important, the RF algorithm builds adaptably within this stage as it is the highest accuracy compared with the other algorithms. Figure 3 shows the proposed method for discovering malicious behavior. As mentioned, we used a feature selection strategy with different types of feature selection methods in the proposed system (within the first phase-IDS) after preprocessing (integer encoding) the results were decreased. For this, the proposed system is not implemented feature selection in this phase.

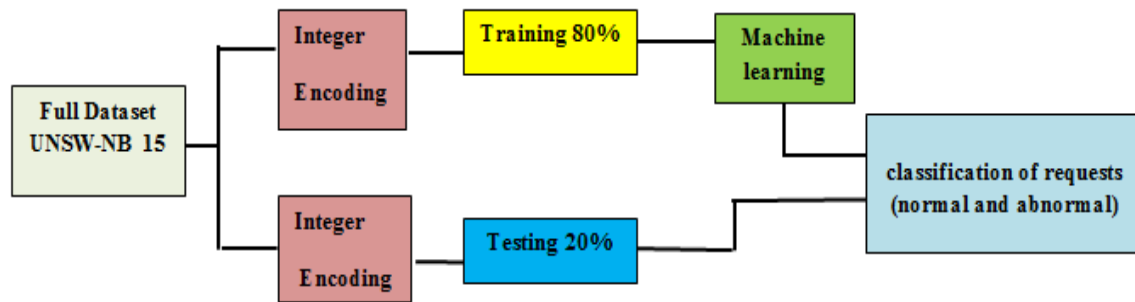


Figure 3. The proposed classification of normal and malicious behavior model

2.2. Classification data with machine learning

The proposed system in the second phase is based on the four sub-phases to deal with the text data in the BBC news data set, which are sorted as follows: i) load BBC dataset, ii) pre-processing, iii) feature extraction, and iv) classification. The proposed system uses on BBC news datasets as: British Broadcasting Corporation (BBC) news data set “<https://www.bbc.com/news>” is in the form of raw text documents and contains 2225 text files that obtained from website of BBC news identical to events in five local regions in the time between 2004 and 2005. These documents are arranged into 5 folders named with the class label as (entertainment, business, sport, politics, and tech) and each of them contains new articles related to that class label.

2.3. Pre-processing

Preprocessing is a very important step which is done to get a better quality input that is performed by tokenization and removing stop words. The main advantage of preprocessing is cleaning and arranging the text to be classified. For the proposed BBC dataset: each folder contains many documents corresponding to each article stored from the directory names of the dataset (the articles related to business are inside the folder name ‘business’). After that, each category is labeled as id (business:0, entertainment:1, politics:2, sport:3, tech:4). Table 1 shows the distribution of categories in this data set is as follows:

Category	ID	Number of items	Cryptography algorithm
Business	0	510	AES
Entertainment	1	386	RC4
Politics	2	417	AES
sport	3	511	Nothing
Tech	4	401	3DES

The classification phase is based on different steps explained in Figure 4, which contains the data pre-processing, feature extraction and model training-testing phases of the ML classifier. The pre-processing datasets are applied due to reasons: 1) reducing the dataset size to get hold of the best efficient data analysis, 2) making dataset adaptable to provide a better analysis selection method. Also, the goal of feature extraction step is to decrease the dimensions of the dataset by omitting characteristics which are not related to the categorization [12].

$$weight_{x,y} = \begin{cases} \log(tf_{x,y} + 1) \log \frac{c}{z_x} & \text{if } tf_{x,y} \geq 1 \\ 0 & , \text{ otherwise} \end{cases}$$

Here, $tf_{x,y}$ is the recurrence of term x in document y , c is the count of documents in the text gathering and z_x is the count of documents where term x manifests.

As mentioned before, the classification features are based on two phases as follows:

- The request validation phase: it is used to (check and validate normal request or abnormal requests).
- The classification phase: it is a significant stage, whose goal is to categorize the invisible news to their respective classes.

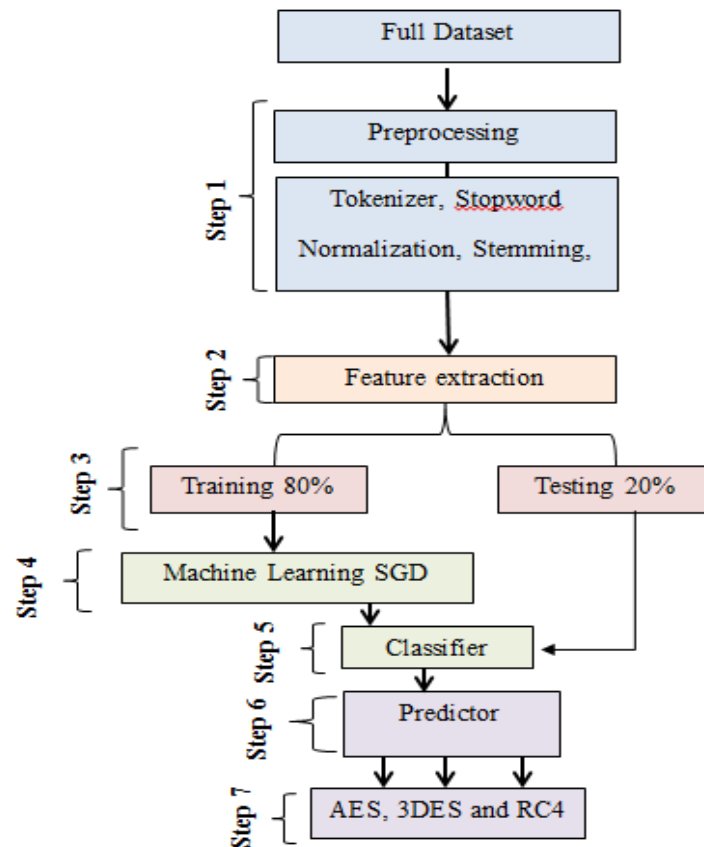


Figure 4. The data classification phase block diagram

The data preprocessing is based on the following strategies:

- Tokenizer; the first step is to divide the text to suitable units (words or letters or expressions). The units named as tokens.
- Stop word removal; it is an efficient way in text preprocessing, which use natural language processing (NLP), its main work is to remove meaningless and useless words to get a more useful text document. Dataset dimensions are reduced based on stop-words. In that case, the remaining keywords within the dataset can be identified depending on the extraction automatic feature methods.
- Normalization; in this step, all words are organized and united in lower case form, which means all upper case forms will be transformed to lower case, removing samples such as numbers.

- d. Stemming; the proposed system uses a stemming process to eliminate any suffixes or prefixes from the word and to return it to its origin or root. Here, snow ball stemming type is used.

3. METHOD

ML techniques have been adopted in the two phases of the proposed approach; the first phase is to classify requests destined for the cloud and to build a model for intrusion detection that targets the private cloud and then to analyze the requests whether they have normal behavior or malicious behavior. This classifier has been trained by relying on this phase on the UNSW-NB15 dataset. Next: the second phase which aims to classify the data to be stored in the cloud based on the importance (sensitivity) of data as follows: top secret (highly confidential), confidential, and standard data (basic data). Then these three types are encrypted in the server as three types (AES, 3DES, and RC4). The proposed system is based on the two ML algorithms as follows:

3.1. Random forest

The main steps of RF working steps are: i) selecting the random samples from a dataset, ii) creating a DT for each sample and getting a prediction result from each DT, iii) performing a specific vote for each result predicted, and iv) selecting the prediction result with the most votes as the final prediction.

3.2. Stochastic gradient descent learning

The proposed system is based on the stochastic gradient descent (SGD) learning as the second method, which replaces the actual gradient that is calculated from the entire proposed dataset by estimating calculated values from a randomly selected subset of the data. In such a manner where high-dimensional optimization problems are available, the algorithm provides less computational power (as the number of resources required to run), and it achieves faster iterations in trade for a lower convergence rate procedure of SGD.

4. RESULTS AND DISCUSSION

The proposed approach is based on configuring a server that acts as a third party between the user and the cloud to secure protection between the two parties. It uses ML and encryption techniques to protect the cloud and the data stored within the private cloud. In the first phase, to detect the attacks, we train the classifier using “UNSW-NB15” dataset. In addition, the BBC News dataset was adopted for the second phase to category the data. In the first phase, the Naive Bayes, SGD, LR, KNN, RF, and DT algorithms were tested.

The method of classifying data based on the proposed ML algorithms is divided into two main processes, namely the data training process and the testing process. The performance comparison parameters used as precision, accuracy, recall, and F1-score, which they based on some of the following [13]:

- a. True-positive (TP), represents the positive examples that are properly classified [14].
- b. False-negative (FN), represents the positive examples that are incorrectly classified.
- c. False-positive (FP), denotes the negative examples that are incorrectly predicted and classified.
- d. True-negative (TN), denotes the negative instances that are properly predicted by the classifier [15].

The evaluation metrics were defined based on the confusion matrix, as shown in (1) to (5).

- a. Precision is the number of TP divided by the number of TP multiple by FP. The precision can be computed based on (1) [16].

$$\text{Precision} = \frac{TP}{TP+FP} \quad (1)$$

- b. Accuracy is the number of correct predictions, which is divided by the total number of predictions. The accuracy can be computed based on (2) [17].

$$\text{Accuracy} = \frac{TP + TN}{TP+TN+FP + FN} \quad (2)$$

- c. Recall is the number of TP divided by the number of TP multiple by the number of FN, as show in (3) [18].

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

d. F1-score, is also called a f1-score or the f1-measure, it is the result of $2*((precision*recall)/(precision+recall))$, as shown in (4) [19].

$$F1 - score = \frac{(2*TP)}{(2*TP+FN+FP)} \tag{4}$$

e. Detection rate (DR) is defined as the ratio of correct positive predictions to the total number of positive predictions, as shown in (5) [20], [21].

$$DR = \frac{TP}{TP+FN} \tag{5}$$

f. False alert rate (FAR) and false positive rate (FPR), represents the proportion of negative predictions; this is considered as positive-anomaly-for all negative predictions. The lower value is the better. This metric shown in (6) [22], [23].

$$FAR = \frac{FP}{FP+TN} \tag{6}$$

g. Error rate: it can be defined as the number of all wrong predictions divided by the entire number of the dataset [24], [25].

h.

$$ERR = \frac{b+c}{a+b+c+d} \tag{7}$$

The result file of the used algorithms is shown in Table 2 and Figure 5. The RF algorithm and DT algorithm provide better results from the point of accuracy, detection rate, building algorithm, and so on compare with other algorithms and the RF algorithm is considered the best in terms of speed as it depends on randomness.

Table 2. The results of the algorithms used Phase 1

Parameters		SGD	NB	RF	DT	LR	KNN
Weighted	Precision	0.78	0.80	1.00	1.00	0.89	0.90
Avg	Recall	0.76	0.74	1.00	1.00	0.85	0.89
	F1-Score	0.75	0.73	1.00	1.00	0.86	0.89
	FAR	0.4134	0.4408	0.00	0.0	0.1005	0.1317
	DR	0.9145	0.9526	1.00	1.00	0.8354	0.9019
	Accuracy	0.76	0.74	1.00	1.00	0.85	0.89

This paper shows that the efficiency of SGD and LR are the best for analyzed datasets due to the ease and simple of implementation and fast training model. In other words, SGD converts dataset attributes into groups of relational attributes and then classified them based on this point for this the execution time is less. While the LR deals with the overall dataset attributes which lead execution time is large and the accuracy is the same for both of them. Figure 5 shows the result from the proposed phase 2.

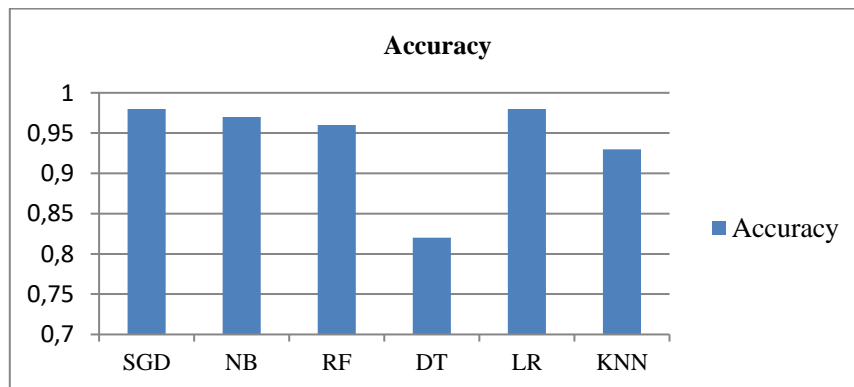


Figure 5. The results of algorithms used phase 2

5. CONCLUSION





In this paper, a secure private cloud using ML and cryptography is proposed. The experimental evaluations were performed on two datasets for different purposes: UNSW-NB15 of the normal-attack dataset and the BBC classification dataset. The proposed method is adopted to encrypt the non-attack data securely and reduce the over-processing consumption of the differed data by making multi encryption levels according to the importance of the data.

Phase one of the proposal which detects normal and attacks flow does provide better results in the case of the ML algorithm of RF which is adopted from among many ML algorithms. The study shows that the accuracy of the RF algorithm is 100%. Thus, the best for the first analyzed phase is RF. In addition, the high accuracy of the second analyzed phase is 98% from the SGD learning algorithm to classify different data categories.





REFERENCES

- [1] S. Goyal, "Public vs private vs hybrid vs community-cloud computing: a critical review," *Int. J. Comput. Netw. Inf. Secur.*, vol. 6, p. 20, 2014.
- [2] Z. Masetic, K. Hajdarevic, and N. Dogru, "Cloud computing threats classification model based on the detection feasibility of machine learning algorithms," *2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2017 - Proc.*, pp. 1314–1318, 2017, doi: 10.23919/MIPRO.2017.7973626.
- [3] Z. He, T. Zhang, and R. B. Lee, "Machine Learning Based DDoS Attack Detection from Source Side in Cloud," *Proc. - 4th IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2017 3rd IEEE Int. Conf. Scalable Smart Cloud, SSC 2017*, pp. 114–120, 2017, doi: 10.1109/CSCloud.2017.58.
- [4] A. L. G. S. Mahmood, "Data Security Protection in Cloud Computing by using Encryption," *Kirkuk Univ. Journal/Scientific Stud.*, vol. 12, no. 4, pp. 849–1992, 2017.
- [5] R. Kolli, S. Mile, S. Shetty, S. J. B, and C. BM, "Improved Data Security Protection Mechanism for Cloud Storage using Two Factors," *Ijarcece*, vol. 6, no. 5, pp. 24–29, 2017, doi: 10.17148/ijarcece.2017.6505.
- [6] Z. Mašetić, D. Kečo, N. Dođru, and K. Hajdarević, "SYN flood attack detection in cloud computing using support vector machine," *TEM J.*, vol. 6, no. 4, pp. 752–759, 2017, doi: 10.18421/TEM64-15.
- [7] M. M. Sakr, M. A. Tawfeeq, and A. B. El-Sisi, "Network Intrusion Detection System based PSO-SVM for Cloud Computing," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 3, pp. 22–29, 2019, doi: 10.5815/ijcnis.2019.03.04.
- [8] K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D. G. Narayan, "Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 2297–2307, 2020, doi: 10.1016/j.procs.2020.03.282.
- [9] A. R. Wani, Q. P. Rana, and N. Pandey, "Machine Learning Solutions for Analysis and Detection of DDoS Attacks in Cloud Computing Environment," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 3, pp. 2205–2209, 2020, doi: 10.35940/ijeat.b3402.029320.
- [10] G. K. Shyam and S. Doddi, "Achieving Cloud Security Solutions through Machine and Non-Machine Learning Techniques: A Survey," *J. Eng. Sci. Technol. Rev.*, vol. 12, no. 3, 2019.
- [11] J. Joseph and J. R. Jeba, "Information extraction using tokenization and clustering methods," *Int. J. Recent Technol. Eng. (IJRTE)*, vol. 8, no. 4, pp. 3690–3692, 2019, doi: 10.35940/ijrte.D7943.118419.
- [12] I. S. I. Abuhaiba and H. M. Dawoud, "Combining different approaches to improve arabic text documents classification," *Int. J. Intell. Syst. Appl.*, vol. 9, no. 4, p. 39, 2017, doi: 10.5815/ijisa.2017.04.05.
- [13] X. Li, P. Yi, W. Wei, Y. Jiang, and L. Tian, "LNNLS-KH: A Feature Selection Method for Network Intrusion Detection," *Secur. Commun. Networks*, vol. 2021, p. 8830431, 2021, doi: 10.1155/2021/8830431.
- [14] V. Kumar, D. Sinha, A. K. Das, S. C. Pandey, and R. T. Goswami, "An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset," *Cluster Comput.*, vol. 23, no. 2, pp. 1397–1418, 2020, doi: 10.1007/s10586-019-03008-x.
- [15] U. Vora, J. Mahato, H. Dasgupta, A. Kumar, and S. K. Ghosh, "Machine Learning–Based Security in Cloud Database—A Survey," *Mach. Learn. Tech. Anal. Cloud Secur.*, pp. 239–269, 2021, doi: 10.1002/9781119764113.ch12.
- [16] N. Pandeewari and G. Kumar, "Anomaly detection system in cloud environment using fuzzy clustering based ANN," *Mob. Networks Appl.*, vol. 21, no. 3, pp. 494–505, 2016, doi: 10.1007/s11036-015-0644-x.
- [17] G. Uçtu, M. Alkan, İ. A. Dođru, and M. Dörterler, "A suggested testbed to evaluate multicast network and threat prevention performance of Next Generation Firewalls," *Futur. Gener. Comput. Syst.*, vol. 124, pp. 56–67, 2021, doi: 10.1016/j.future.2021.05.013.
- [18] B. S. Al-Attab and H. S. Fadewar, "Hybrid data encryption technique for data security in cloud computing," *Sinhgad Inst. Manag. Comput. Appl.*, 2018, pp. 221–224.
- [19] A. S. Anakath, S. Rajakumar, and S. Ambika, "Privacy preserving multi factor authentication using trust management," *Cluster Comput.*, vol. 22, no. 5, pp. 10817–10823, 2019, doi: 10.1007/s10586-017-1181-0.
- [20] D. Hong, J.-K. Lee, D.-C. Kim, D. Kwon, K. H. Ryu, and D.-G. Lee, "LEA: A 128-bit block cipher for fast encryption on common processors," in *international workshop on information security applications*, 2013, pp. 3–27, doi: 10.1007/978-3-319-05149-9_1.
- [21] D. Delen and M. D. Crossland, "Seeding the survey and analysis of research literature with text mining," *Expert Syst. Appl.*, vol. 34, no. 3, pp. 1707–1720, 2008, doi: 10.1016/j.eswa.2007.01.035.
- [22] H. Kamel and M. Z. Abdullah, "Distributed denial of service attacks detection for software defined networks based on evolutionary decision tree model," *Bull. Electr. Eng. Informatics*, vol. 11, no. 4, pp. 2322–2330, 2022, doi: 10.11591/eei.v11i4.3835.
- [23] A. K. Singh and D. Saxena, "A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment," *J. Appl. Secur. Res.*, vol. 17, no. 3, pp. 385–412, 2022.
- [24] A. J. Altamemi, A. Abdulhassan, and N. T. Obeis, "DDoS attack detection in software defined networking controller using machine learning techniques," *Bull. Electr. Eng. Informatics*, vol. 11, no. 5, pp. 2836–2844, 2022, doi: 10.11591/eei.v11i5.4155.
- [25] K. F. Hassan and M. E. Manaa, "Detection and mitigation of DDoS attacks in internet of things using a fog computing hybrid approach," *Bull. Electr. Eng. Informatics*, vol. 11, no. 3, pp. 1604–1613, 2022, doi: 10.11591/eei.v11i3.3643.

BIOGRAPHIES OF AUTHORS

Ali Abdulsattar Jabbar     he studied at the university of Babylon, college of Information Technology, Networks department and completed master's degree in 2021. He interested with network security, cloud threats, attacks and solutions, cloud security solutions through machine learning techniques, cloud attacks solutions through intrusion detection system (IDS), and cloud security solutions through cryptography. The main research topic is secure private cloud using machine learning and cryptography. He can be contacted at email: ali.jabbar@student.uobabylon.edu.iq.



Wesam Sameer Bhaya     Ph.D. in Computer Science. He is a Professor in the Faculty of Information Technology, Information Security Department, University of Babylon, Iraq. The current areas of interest are information networking and information security. He can be contacted at email: wesambhaya@uobabylon.edu.iq.