SN Computer Science (2022) 3:451
https://doi.org/10.1007/s42979-022-01304-9

ORIGINAL RESEARCH

Investigation of Cybersecurity Attacks and Threats on Cloud Using Black Widow Algorithm with Recurrent Neural Network

S. Senthil Kumar[1] · S. Arockia Panimalar[2] · A. Krishnakumar[3] · M. Prakash[2]

Received: 19 May 2022 / Accepted: 2 July 2022 / Published online: 20 August 2022

Abstract
The amount of personal and sensitive information collected by data collectors is rising. Those details are processed and saved on the cloud's servers. Risks and hazards exist in the cloud infrastructure. The amount of data stored on the cloud is enormous, and some of it is secret or personal, making it vulnerable to a breach or attack. In this case, a strong security solution was required to secure the data from hackers and eavesdroppers. In the field of cloud computing, anomalies and insider assaults will deactivate service providers, resulting in the entire system failing. Insider assaults and infiltration are difficult to handle with traditional network defensive measures. The anomaly identification approach is created in this study to determine the incidence of attack, and the proposed approach uses black widow algorithm for feature selection whereby the classification is attained using recurrent neural network (RNN). The process of feature selection will eliminate the redundant features and the significant features are retrieved using meta-heuristic technique. The selected features are utilized for classification using RNN. The feature selection highly helps the process of classification and it enhances the accuracy of the classification. The classification process is simplified by the feature selection process and the training error is minimized by the RNN technique. The use of a neural network to effectively identify features improves classification accuracy. The RNN's performance investigation and outcomes categorize real-time threats in the cloud environment with high accuracy.

Keywords Cloud · Cyber-attack · Security · Optimization · Feature · Deep learning · Neural network · Classification

Introduction

Many of the most significant innovations that have captivated the interest of engineers all around the universe are cloud computing. While it provides many benefits, like scalability, fast adaptability, measurable capabilities, and, most importantly, the possibility for cost reductions for businesses, it also comes with its own unique of security dangers that no company can afford to ignore [1]. Due to the vast variety of dangers inherent in every Cloud computing system and the lack of credible security advice, businesses are reluctant to accept cloud computing from an otherwise favorable environment [2, 3].

At its most basic level, Cloud Computing isolates info and application properties from the core structure and method utilized to provide them, with the integrating allocation of resources based on a functional description and elasticity. Cloud computing improves collaboration, scale, dependability, and agility while also lowering costs for consumers and businesses [4]. To put it another way, Cloud Computing refers to the utilization of a combination of applications,

This article is part of the topical collection "Predictive Artificial Intelligence for Cyber Security and Privacy" guest edited by Hardik A. Gohel, S. Margret Anouncia and Anthoniraj Amalanathan.

S. Senthil Kumar
szenthilkumar@gmail.com

S. Arockia Panimalar
spanimalar21@gmail.com

A. Krishnakumar
krishna2c@gmail.com

M. Prakash
powermprakash@gmail.com

1 Department of Information Technology, Nehru Arts and Science College, TM Palayam, Tamil Nadu, Coimbatore, India

2 Department of Computer Applications, Nehru Arts and Science College, TM Palayam, Coimbatore, Tamil Nadu, India

3 Department of MCA, Sree Saraswathi Thyagaraja College, Tamil Nadu, Pollachi, Coimbatore, India

data, and infrastructure, as well as network, data, and storage resources, and finally distributed services. Exploiting a utility model for allocation, deallocation, and ingesting, these mechanisms may be easily structured, armed, employed, and deconstructed [5].

While Cloud Computing offers tremendous benefits to people and enterprises, likely scalability, adaptability, evaluated services, and multi-tenancy, through automated processes, virtual presence, and accessibility of services, equipment, and apps, there have appeared recently a count of serious risks, including information security, data security for preserving the confidentiality and anonymity of personal data, acquiring and maintaining data, and application security. Larger businesses are unsure if their bulk data will be safe while being transmitted over the internet [6, 7].

Security and risk assessment would include an examination of the impact of different risks and assaults on many components of cloud computing, such as cloud computing adaptability, personal data confidentiality and privacy, and data access and updating [1, 8]. As a result, establishing the most effective solution guidelines for increasing cloud security and privacy has become vital for all cloud-based organizational activities [9, 10]. As a result, reviewing cloud networks to identify the unique security risks and vulnerabilities is critical and necessary [2, 11].

In another way, Cloud Computing is widely used, an evaluation of vulnerabilities and assaults also done, as well as the identification of applicable solution directions to increase security and privacy in the Cloud environment, is a must [12]. Because Cloud Computing is a novel technique, solutions to threats and vulnerabilities lag behind simply executable assaults, such as Cross-Site Scripting (XSS), man-in-the-middle, Malware, DDoS, DoS, SQL injection, and authentication attacks, among others. To do this, it is necessary to develop time-bound responses to threats and manipulation of cloud risks. This research gap inspired the suggested research project. This article uses deep learning and optimization-based approach for the classification of diverse kinds of attacks [13].

Deep learning (DL) is a new field of computer intelligence that offers new ideas, methodologies, and tools for large-scale data processing. It provides assistance to modern organizations that are confronted with the difficult task of deciding how to make decisions from massively increased data to study their markets, clients, distributors, processes, clinical issue identification, and internal operations, among other things. Artificial neural networks (ANN) that are modeled after the structure of neurons in the human brain, which are used in Deep Learning (DL). Although its meaning has varied over time, the term "deep" is used to characterize the presence of several layers in an artificial neural network (ANN). While 10 layers were considered acceptable 5 years ago, currently it is more typical to consider a network to be deep when it contains hundreds of levels [14].

DL is a paradigm change in the very small set of innovative approaches that have been successfully applied to multiple varied fields (image, text, video, audio, and vision), greatly enhancing prior state-of-the-art outcomes produced over decades of years. The greater availability of training data and the relatively inexpensive cost of GPUs for extremely efficient numerical computation are additional factors in DL's success. Deep learning algorithms are used by Google, Microsoft, Amazon, Apple, Facebook, and many more companies on a daily basis to analyze vast volumes of data. This type of competence, on the other hand, is no longer restricted to pure academic research and huge corporations [15].

The remainder of the article is organized as follows: the review of literature is given in Sect. 2, the proposed feature selection with classification is given in Sect. 3, the outcome of the proposed attack detection model is discussed with graphical illustration in Sect. 4, and the article is concluded in Sect. 5.

Literature Review

In the literature, several rule induction and decision tree techniques have been proposed. The Naive Bayes method [16] is a probabilistic classifier, which implies a variable's influence on a particular class is independent of the value of another variable. Class conditional independent is the term for this condition. One of the most well-known and often used categorization methods is the decision tree. The C4.5 algorithm [17] is the most widely used tree classifier. The ID3 (Iterative Dichotomiser 3) algorithm is used to determine a compact decision tree. C4.5's decision tree may be used to classify data, and it's generally referred to as a statistical classifier. The C4.5 method [18], is a landmark of decision tree program that is perhaps the machine learning algorithm that is most commonly used in practice [19]. The distance among the cluster data point and the centroid determines how data points are assigned to clusters in K-Mean Clustering [20].

The k-NN (k-Nearest Neighbors) method [21] is a similarity-based learning method that has been shown to be very successful in a variety of problem areas, including classification. SVM (Support Vector Machines) [22] is the most used approach for machine learning problems in regression and classification. Not only can SVM be used to solve classification difficulties, but it can also be used to solve prediction issues. FCM Clustering (Fuzzy C-Means Clustering) [23] is a clustering approach that permits a single piece of datum to belong to many clusters. In pattern classification, this strategy is commonly employed. The Neural Networks (NNs) [24] are mathematical models of the human brain's operation. Recognition system, image compressing, stock market analysis, medicine, digital nose, defense, and credit applications are only a few types of NN applications mentioned in the literature [25].

Anomaly detection typically employs machine learning techniques [26]. They have gotten a lot of attention from intrusion detection experts as a way to solve the flaws in knowledge base protection systems. C4.5 is more stable than k-NN, according to an experiment conducted by [27]. Another study using three intrusion prevention models based on Multi-Layer Perceptron (MLP), C4.5, and SVM classifiers [28] found that C4.5 is the best technique in terms of detection accuracy and training time, with a rate of 95% (99.05 percent). As a result, in our suggested model, we use the C4.5 algorithm to detect DDoS assaults. The deep learning method is also used to classify various attacks with high accuracy [29].

The existing machine learning approaches necessitate vast data for the purpose of training and susceptible to error rate. The interpretation of outcome is tedious and the process of handling vast data with diverse nature is complicated. Occurrence of redundant features can degrade the performance of classification and the unwanted features utilizes the resources. By considering these drawbacks, an effective approach is framed with optimization and deep learning technique. The significant features are retrieved using black widow optimization (BWO) technique and the classification is attained using recurrent neural network (RNN).

Proposed Methodology

This section discusses about the proposed methodology and the entire process of classification is detailed. Initially, feature selection is done using black widow optimization (BWO) technique and the prominent features are passed to the classification phase.

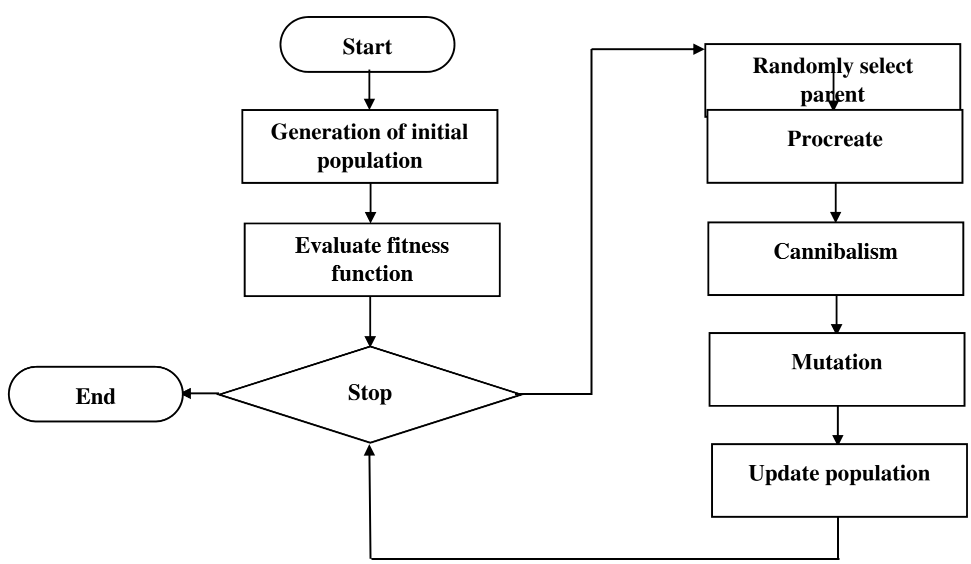
Feature Selection

Spiders are a class of arthropods that include a broad range of other creatures and come in a variety of sizes and shapes. Black widow spiders may be spotted in plains, slopes, and farmland, as well as behind rocks, dried wheat and vegetation stems. The toxicity of a black widow's spider is significantly more lethal than that of a viper, according to assessments. Female black widow spiders live individually, but when they mate, they may approach and mate with one another. After mating, the female spider eats the male spider that is smaller than the female or widow spider.

This spider's matting behavior might be owing to the fact that the female species feels hungry after giving birth, or it could be that by eating the male kind, the father's genetic information is passed on to the young. The black widow optimization technique was created by modeling the behavior of this species of spider in terms of reproduction and devouring. Production, species eating (cannibalism), and mutation are all essential processes in this algorithm.

Figure 1 shows a flowchart of the basic steps in BWO. In the first phase of the BWO process, an initial random set is generated, and every member is evaluated utilizing the objective function that is determined by their fitness value. A counter maintains a track of iterations involved in black widow optimization technique and one unit is introduced to

Fig. 1 Flowchart of proposed approach



the counter every time. The population is then exposed to three rounds of production, cannibalism, and mutation, following which the BWO technique updates the position of every solution. In the last iteration, the most optimal choice is picked as the issue's best solution.

According to Eq. (1), every solution of the issue is regarded a black spider in the BWO process and has the subsequent N_{var} and nPop is at the earliest stage of development. In the global optimization space, these solutions first produce a random value by

$$widow = (w_1, w_2, w_3, \ldots \ldots, w_{N_{var}}) \tag{1}$$

Numerous eggs are generated at every stage of the algorithm, and only a very few them survive, which are more worthy, while the others are discarded. Assume there are two parents, p_1 and p_2, who have coition and produce two new answers, a_1 and a_2, which are generated using Eq. (2) and (3), respectively

$$a_1 = \alpha.p_1 + (1 - \alpha).p_2 \tag{2}$$

$$a_2 = \alpha.p_2 + (1 - \alpha).p_1 \tag{3}$$

The cannibalism step is conducted in three variants in this method. The mother solution that is more suitable, first eliminates the male species, and then the species is consumed among some of the children, and the weaker solutions are removed. Solutions that are more deserving of the parent will induce the parent to consume and eliminate it in the following phase of cannibalism. When it comes to mutations, it is thought that certain spiders have modified some of their parents' characteristics, which is why mutations is employed. The process is illustrated in Fig. 2.

Classification

The feature W is taken as input for Deep RNN classifier for identifying frauds. The Deep RNN scheme is the sequential network architecture, which comprised hidden recurrent layers in system hierarchy. On the other side, it is more effectual and proficient to indicate some function than other classifiers. Here, recurrent association is available among hidden layers. The Deep RNN performs the detection process efficiently based on the series of data. The result of preceding state is considered as input to next state along with hidden information. After that, the recurrent feature computes the

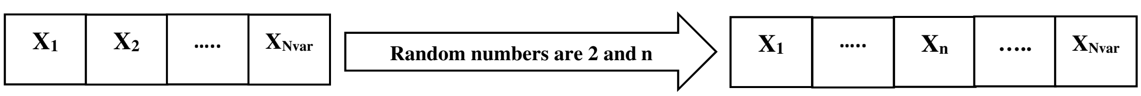


Fig. 2 Mutation process in BWO technique

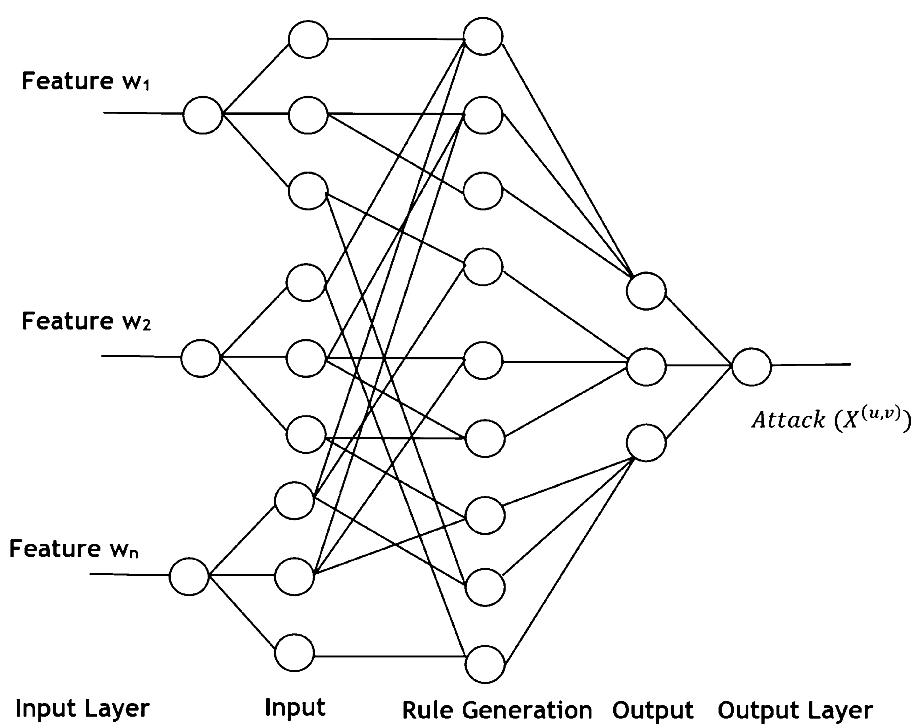


Fig. 3 Architecture of Deep RNN

classifier so as to produce the optimal result. Figure 3 illustrates the architecture of proposed Deep RNN.

The Deep RNN structure is designed through input vector of u^{th} layer at v^{th} period as, $C^{(u,v)} = \{C_1^{(u,v)}, C_2^{(u,v)}, \ldots \ldots C_y^{(u,v)}, C_w^{(u,v)}\}$ and output vector is illustrated as $X^{(u,v)} = \{X_1^{(u,v)}, X_2^{(u,v)}, \ldots \ldots X_y^{(u,v)}, X_w^{(u,v)}\}$. The couple of each component in output and input vectors is denoted as unit. Here, y indicates arbitrary element integer of u^{th} layer also w signified entire number of units in u^{th} layer. Here, except from input and output parameters, random component integer of $(u-1)^{th}$ layer is termed as d an entire quantity of $(u-1)^{th}$ layer is denoted as V. Furthermore, the input spread weight from $(u-1)^{th}$ layer to u^{th} layer is indicated as $\mu^u \epsilon \chi^{w \times V}$ and recurrent weight of u^{th} layer is described as $U^u \epsilon \chi^{w \times w}$. The set of weights is signified as χ and elements of input layer are technically represented as below Eq. (4).

$$C_y^{(u,v)} = \sum_{c=1}^{V} \lambda_{yc}^u X_c^{(u-1,v)} + \sum_{y'}^{w} \theta_{yy'}^u X_{y'}^{(u,v-1)} \tag{4}$$

where, y' designates arbitrary element of u^{th} layer also λ_{yc}^u and $\theta_{yy'}^u$ demonstrate components of μ^u and U^u. The factors of output vector in u^{th} layer are characterized as (Eq. (5)):

$$X_y^{(u,v)} = \eta^u (C_y^{(u,v)}) \tag{5}$$

where, η^u signifies activation function. Moreover, activation function, named as Rectified Linear Unit function (ReLU) as, $\eta(C) = \max(C, \varepsilon)$, sigmoid function as, $\eta(C) = \tanh(C)$ as well as, logistic sigmoid function, $\eta(C) = \frac{1}{(1+e^{-c})}$ are normally used activation function. Let us consider, ε^{th} weight as $\lambda_{y\varepsilon}^u$ and ε^{th} unit as$X_\varepsilon^{(u-i,v)}$, to compose detection procedure simpler, and thus, bias is illustrated as follows (Eq. (6)):

$$X^{(u,v)} = \eta^u \left[\mu^u X^{(u-1,v)} + U^u . X^{(u,v-1)} \right] \tag{6}$$

where, output of classifier is specified by $X^{(u,v)}$.

Table 1 Dataset Description

Dataset Name	Features	Types of Attacks	Attacks utilized for testing
KDDcup 1999	41	22	17
NSL-KDD	41	24	38
UNSW-NB15	49	9 family of attack	9 family of attack

Results and Discussion

This section discusses the dataset description and the performance proposed approach whereby comparison is accomplished to identify the effective approach.

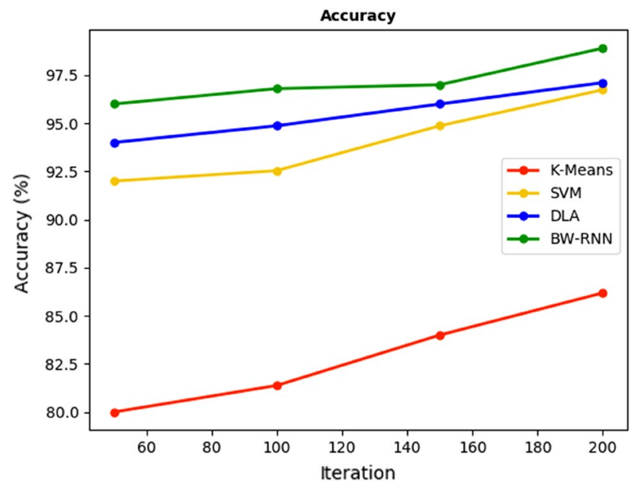


Fig. 4 Comparison of Accuracy

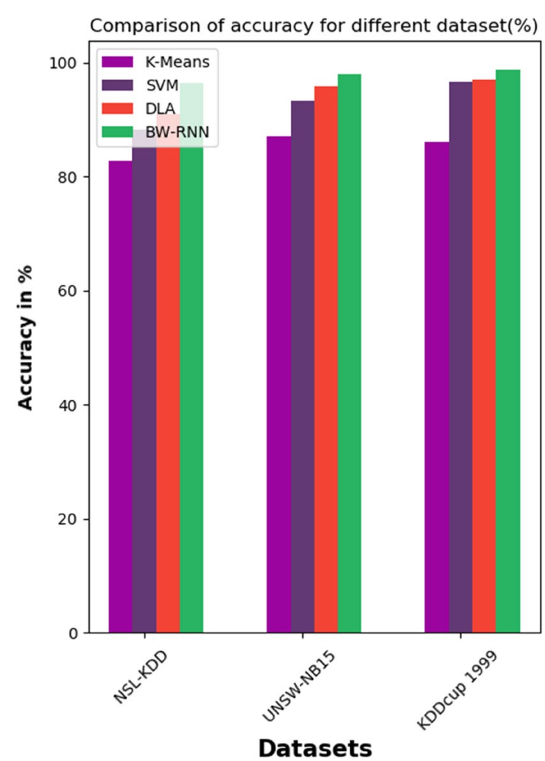


Fig. 5 Comparison of Accuracy for Different Dataset

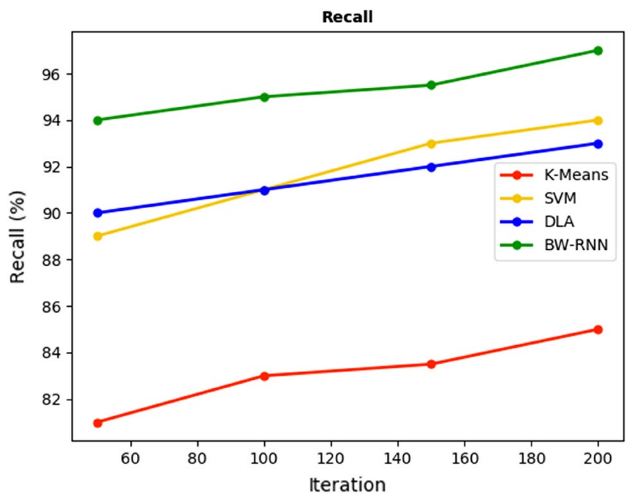


Fig. 6 Comparison of Recall

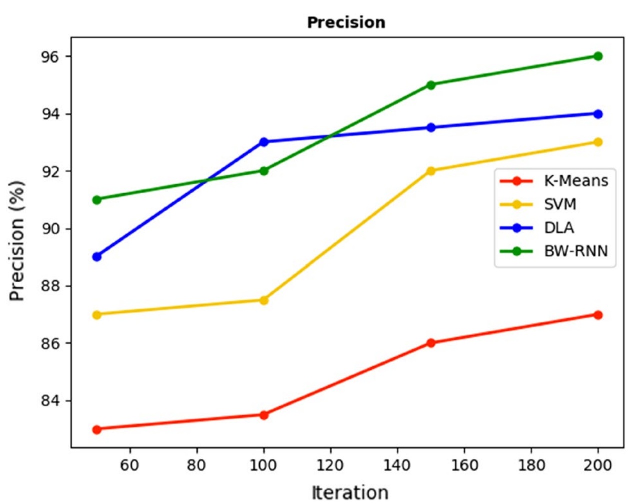


Fig. 7 Comparison of Precision

Dataset description

To validate the accuracy of the deep learning-based cyber-attack forecasting system over cloud, the research utilizes three empirical publicly accessible datasets. The description of the dataset is given in Table 1.

Investigation of classification performance

Accuracy

The closeness of the determine truths from the categorized examples is defined by accuracy (Figs. 4, 5, 6, 7, 8, 9). The presentation of statistical bias and systematic flaws is known as correctness. It is also the identification (both TP and TN

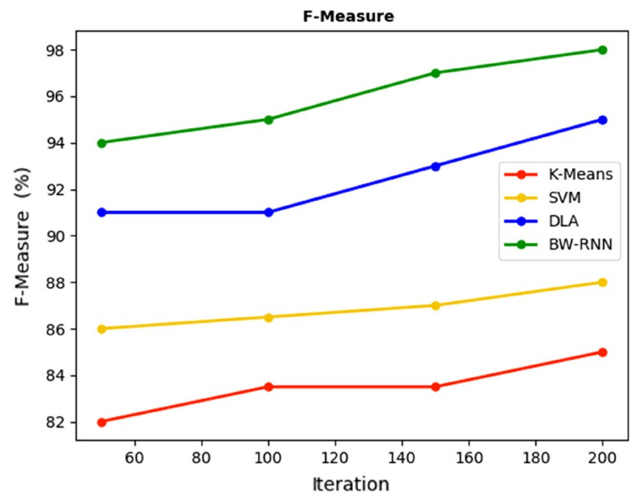


Fig. 8 Comparison of F-Measure

values) among the count of the assessed classes, as well as the proximity of an approximation to the genuine value. When the least accuracy occurs, the resultant and real resultant values differ. It is the proportion of correctly detected instances to the total number of occurrences examined. Table 2, 3, 4, 5, 6 represents the occuracy and results which is correctly detected instances to the total number of occurrences examined. It is calculated as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Recall

The recall is the fraction of related instances among the actually reclaimed instances. The recall is an estimation measure of successful prediction rate and the count of related results is returned as recall. It is measured based on the detection of TP and False Negative (FN) rates. It is calculated as:

$$Recall = \frac{TP + TN}{TP + FN}$$

Precision

The closeness of the measurement and the importance among the values discovered are shown by the positive analytical value or precision. Random mistakes are expressed as precision, which is calculated using statistical factors. Precision and accuracy are phrases that are interchangeable. It is calculated as:

Fig. 9 Comparison of Attack Detection Time

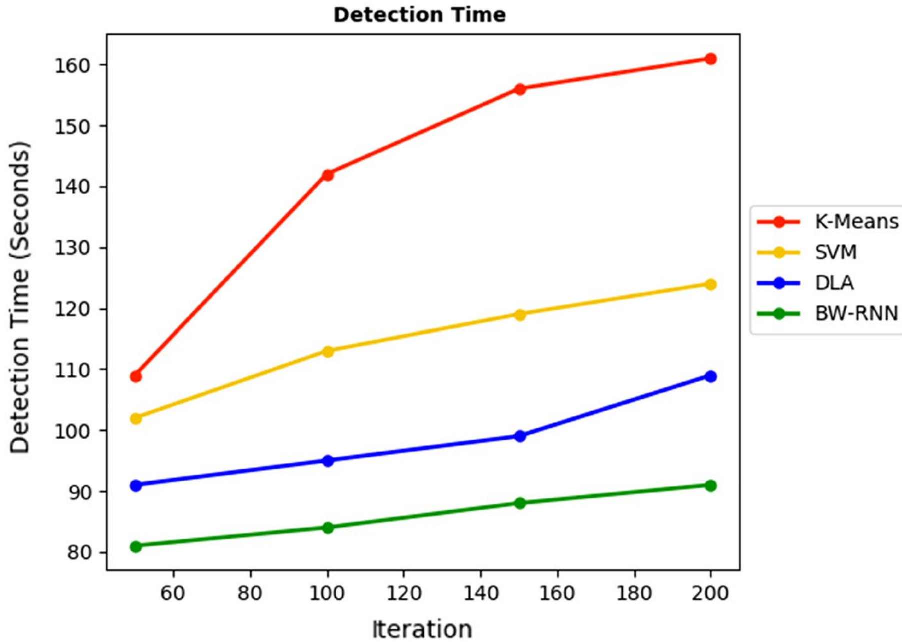


Table 2 Comparison of Accuracy

Iteration	K-Means	SVM	DLA	BW-RNN
50	80	92	94	96
100	81.38	92.54	94.87	96.8
150	84	94.87	96	97
200	86.19	96.74	97.11	98.9

Table 3 Comparison of Accuracy for Different Dataset

Iteration	K-Means	SVM	DLA	BW-RNN
NSL-KDD	82.78	88.32	90.99	96.43
UNSW-NB15	87.05	93.38	95.84	98.13
KDDcup 1999	86.19	96.74	97.11	98.9

Table 4 Comparison of Recall

Iteration	K-Means	SVM	DLA	BW-RNN
50	81	89	90	94
100	83	91	91	95
150	83.5	93	92	95.5
200	85	94	93	97

Table 5 Comparison of Precision

Iteration	K-Means	SVM	DLA	BW-RNN
50	83	87	89	91
100	83.5	87.5	93	92
150	86	92	93.5	95
200	87	93	94	96

Table 6 Comparison of F-Measure

Iteration	K-Means	SVM	DLA	BW-RNN
50	82	86	91	94
100	83.5	86.5	91	95
150	83.5	87	93	97
200	85	88	95	98

Table 7 Comparison of Attack Detection Time

Iteration	K-Means	SVM	DLA	BW-RNN
50	109	102	91	81
100	142	113	95	84
150	156	119	99	88
200	161	124	109	91

$$Precision = \frac{TP}{TP + FP}$$

F-Measure

F-measure or F-score is stated as an accuracy of test in the problem of classification. To compute F-measure, precision and recall value are taken, whereas precision is the count of the true positive values (positive values or correctly classified values) and the recall is the fraction of related instances among the actually reclaimed instances (sensitivity or classified instances). Otherwise, it is stated as a harmonic mean of the precision value and recall value. F-measure is chiefly used in the multiclass classification problems and it stabilizes both the precision and recall value. It is computed as:

$$F - Measure = \frac{2.Precision.Recall}{Precision + Recall}$$

Detection Time

The time taken to forecast the occurrence of attack over cloud is determined as attack detection time. The attack detection time for different approaches is given in Table 7 and the proposed approach attains minimal attack detection time.

Conclusion

The quantity of data in the cloud is massive, and some of it is sensitive or personal, that is vulnerable to a hack or attack. To protect the data from hackers and eavesdroppers, a strong security solution is required. Anomalies and insider attacks in cloud computing will disable service providers, causing the entire system to collapse. Traditional network defensive mechanisms struggle to deal with insider attacks and penetration. In this paper, an anomaly detection strategy is developed to assess the frequency of attack. The suggested approach employs the black widow algorithm for feature selection, with recurrent neural networks used for classification (RNN). The redundant features are eliminated and the promising features are passed to the classification system. The normal and attack scenario over the cloud is classified by the RNN, which yields accuracy of 98.9% and outperforms other existing approaches.

Authors Contribution The author has contributed the entire work.

Funding The authors declare that they have no known competing financial interests.

Data Availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of Interest The authors declare that there is no conflict of interest.

Informed Consent Informed consent was obtained from all individual participants included in the study.

Informed Consent on Studies with Human and Animal Subjects This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Rashid A, Chaturvedi A. Cloud computing characteristics and services: a brief review. Intern J Computer Sci Eng. 2019;7(2):421–6.
2. Sunyaev A. Cloud computing. Intern computing. 2020. https://doi.org/10.1007/978-3-030-34957-8_7.
3. Alam T. Cloud Computing and its role in the Information Technology. IAIC Trans Sustain Digit Innovation (ITSDI). 2020;1(2):108–15.
4. Butt SA, Tariq MI, Jamal T, Ali A, Martinez JLD, De-La-Hoz-Franco E. Predictive variables for agile development merging cloud computing services. IEEE Access. 2019;7:99273–82.
5. Arpaci I. A hybrid modeling approach for predicting the educational use of mobile cloud computing services in higher education. Comput Hum Behav. 2019;90:181–7.
6. Yang P, Xiong N, Ren J. Data security and privacy protection for cloud storage: a survey. IEEE Access. 2020;8:131723–40.
7. Attaran M, Woods J. Cloud computing technology: improving small business performance using the Internet. J Small Bus Entrep. 2019;31(6):495–519.
8. Patil SS, Chavan R. Cloud business intelligence: an empirical study. Stud Indian Place Names UGC Care J. 2020;27:747–54.
9. Gochhait S, Butt SA, Jamal T, Ali A. Cloud enhances agile software development. In Cloud Computing Applications and Techniques for E-Commerce (pp. 28–49). IGI Global, 2020.
10. Abdalla PA Varol A Advantages to disadvantages of cloud computing for small-sized business. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6): 2019 IEEE.
11. Khan S. Cloud computing: issues and risks of embracing the cloud in a business environment. Intern J Edu Managt Eng. 2019;9(4):44.
12. Song Y Wang H Wei X Wu L Efficient attribute-based encryption with privacy-preserving key generation and its application in industrial cloud. Security and communication networks, 2019
13. Li Z, Shen H, Cheng Q, Liu Y, You S, He Z. Deep learning based cloud detection for medium and high resolution remote sensing images of different sensors. ISPRS J Photogramm Remote Sens. 2019;150:197–212.
14. Ghosh AM, Grolinger K Deep learning: Edge-cloud data analytics for iot. In 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE) (pp. 1-7). 2019; IEEE.
15. Zhang Z, Dai Y, Sun J. Deep learning based point cloud registration: an overview. Virtual Real Intell Hardw. 2020;2(3):222–46.

16. Blum AL, Langley P. Selection of relevant features and examples in machine learning. Artif Intell. 1997;97(1–2):245–71.
17. Quinlan JR (2014) Programs for Machine Learning. ISBN: 9780080500584, Paperback ISBN: 9781558602380. https://www.elsevier.com/books/c45/quinlan/978-0-08-050058-4.
18. Holmes, G., Donkin, A., & Witten, I. H. 1994. Weka: A machine learning workbench. In *Proceedings of ANZIIS'94-Australian New Zealnd Intelligent Information Systems Conference* (pp. 357–361). IEEE.
19. Witten IH, Frank E. Data mining: practical machine learning tools and techniques with Java implementations. ACM SIGMOD Rec. 2002;31(1):76–7.
20. Hartigan JA, Wong MA. Algorithm AS 136: A k-means clustering algorithm. J Royal Stat Soc Ser C (Appl Stat). 1979;28(1):100–8.
21. Keller JM, Gray MR, Givens JA. A fuzzy k-nearest neighbor algorithm. IEEE Trans Syst Man Cybern. 1985;4:580–5.
22. Hearst MA, Dumais ST, Osuna E, Platt J, Scholkopf B. Support vector machines. IEEE Intell Sys Their appl. 1998;13(4):18–28.
23. Bezdek JC, Ehrlich R, Full W. FCM: The fuzzy c-means clustering algorithm. Comput Geosci. 1984;10(2–3):191–203.
24. Haykin S Neural networks and learning machines.[sl] pearson Upper Saddle River. NJ, USA, 3: 2009.
25. Murray AF, editor. Applications of neural networks. Boston: Kluwer Academic Publishers; 1995. p. 157–89.
26. Lane B Poole M Camp M Murray-Krezan J. Using machine learning for advanced anomaly detection and classification. In Advanced Maui Optical and Space Surveillance Tech. Conf. (AMOS): (2016).
27. HM M, Kumar RA. A survey on machine learning techniques used for detection of DDOS attacks (May 17, 2019). *In: Proceedings of the Second International Conference on Emerging Trends in Science & Technologies For Engineering Systems (ICETSE-2019)*. 2019. https://ssrn.com/abstract=3508610.
28. Sheta AF, Alamleh A. A professional comparison of c4 5, mlp, svm for network intrusion detection based feature analysis. Intern Congr glob Sci Technol. 2015;47:15.
29. Nguyen KK, Hoang DT, Niyato D Wang P, Nguyen D, Dutkiewicz E. Cyberattack detection in mobile cloud computing: A deep learning approach. *In: 2018 IEEE WirelessCommunications and Networking Conference (WCNC)*. 2018;1–6. https://doi.org/10.1109/WCNC.2018.8376973.