International Conference on Inventive Computation Technologies (ICICT 2024)
DVD Part Number : CFP24F70-DVD ; ISBN : 979-8-3503-5928-2

An Efficient Investigation of Cloud Computing Security with Machine Learning Algorithm

Dr.R.Senthilkumar
Computer Science and Engineering
Shree Venkateswara Hi Tech Engineering College
Erode,Tamilnadu, India
svhecrsk@gmail.com

Dr.S.Yasotha
Computer Science and engineering
Sri Eshwar College of Engineering
Coimbatore,Tamilnadu, India
yasotha.vlsi@gmail.com

P. M. Manochithra
Computer Science and Engineering
Shree Venkateswara Hi Tech Engineering College
Erode, Tamilnadu, India
manochitra64@gmail.com

J.Senthil
M.Tech Computer Science and Engineering
Sri Krishna College of Engineering and Technology
Coimbatore,Tamilnadu, India
senthilgobi05@gmail.com

Dr.G.Sivakumar
Computer Science and Engineering
Erode Sengunthar Engineering College
Erode,Tamilnadu, India
sivakumarganapathi@gmail.com

***Abstract*—Due to developments in technologies like Cloud Computing (CC), the Internet of Things (IoT), etc., the data volume transmitted across communication infrastructures has skyrocketed recently. In order to make network systems susceptible, attackers have increased their determinations. Improving the security of such network systems is, hence, very crucial. Using Deep Learning (DL) methods, with an intrusion detection system (IDS) framework is put into action in this research. The Gated Recurrent Unit (GRU) as well as Support Vector Machine (SVM) are used in this study for detection of attacks. Therefore, as per the study, in lieu of Softmax in the GRU model's last output layer, this study introduces a linear SVM. The NSL-KDD dataset is taken into account to evaluate the proposed IDS framework's performance. In addition, when the number of features increases, current IDSs have poor test accuracy ratings when it comes to identifying new attacks. Each dataset's feature space was reduced using an XGBoost (XGB)-based feature selection approach in this research. After that, 22 detailed characteristics were selected from the NSL-KDD dataset using XGB. The results show that, as compared to other approaches, the proposed IDS paradigm worked wonders.**

Keywords—Internet of Things, Deep Learning, NSL-KDD dataset, Intrusion Detection System, Support Vector Machine, Gated Recurrent Unit.

I. INTRODUCTION

Recently, a new architecture for facilitating as well as transporting services over the internet has emerged termed as CC. The necessity for data analysis, storage, along with display owing to escalating computing costs and common budgetary constraints has forced significant changes to the current cloud architecture [1]. Machine learning (ML) is one method of cloud security. In order to prevent or detect cyberattacks and security vulnerabilities, ML techniques have been used in several ways. A Systematic Literature Review (SLR) on cloud security methods and techniques using ML is conducted. It tested whether it's for internal use or to provide services to external clients, a large number of companies are investing in this field [2].

The security issues that both CC and the IoT have to deal with. With a particular focus on securing the usage along with transmission of Big Data, these two previously stated technologies (CC and IoT) have been specifically contrasted, investigated, and shown to have advantageous integration features [3]. A hybrid ML (RATS-HM) approach to address such issues by combining resource allocation security with effective job scheduling in CC. The performance of CC can be negatively impacted by inefficient resource management [4].

This work presents an enhanced Self-adaptive evolutionary extreme learning machine (SaE-ELM) based distributed denial of service (DDoS) attack detection system. The SaE-ELM model is enhanced by adding two new characteristics. It is therefore crucial to fight against such assaults [5]. However, there are security and privacy issues when it comes to outsourcing data and business apps to the cloud or a third party, which has made embracing cloud implementation and services essential. To address the current security issues, researchers and impacted organizations have put forth several security measures in the literature. A thorough analysis of CC security and privacy concerns is also provided by the literature [6].

Embedded systems demonstrate exceptional efficacy and efficiency while operating in intricate jobs. The extensive manipulation and selection of empirical technologies is beneficial for the smooth operation of future development. Intellectual Comics is excited to generate graphics connected to a combination of numerous technologies because of the many uses [7]. However, there is a danger of data breaches, , injection vulnerabilities ,account compromises, abusive use of features like trial periods and DDoS attacks when requesting services from the same pool. Innovations in technology have recently pushed users toward cloud-based architectures [8].

Accuracy still suffers from various problems, despite the many proposed methods. This inaccuracy is thought to have resulted from ineffective feature selection. Therefore, in

order to address this study, the following factors are taken into account:

- The dataset is subjected to a feature selection algorithm that is based on XGB.
- The XGB algorithm is well-known for its effectiveness as well as enables the optimisation of differentiable loss functions of any kind.
- Consequently, this study employs this algorithm to get optimised feature significance scores. With the proposed SVM-GRU model for classification, an analysis is provided. Since GRU faces issues with optimization SVM is also used with GRU to tackle this issue.
- Using several performance indicators, a comprehensive analysis of the XGB-DL-IDS framework is carried out.
- Other IDS frameworks are also compared to XGB-DL-IDS.

The reminder of this work is planned as surveys. Section II offers an outline of some current and recent works. The proposed technique is defined in Section III. After a summary of the findings as well as analysis in Section IV, the references are provided.

II. LITERATURE REVIEW

This section provides details regarding some existing approaches that are proposed to detect the intrusions. Table 1 summarizes the ML to detect the intrusions and lists their advantages and disadvantages, so it is able to find all the information needed.

TABLE I. LITERATURE REVIEW

Paper and Author	Method	Advantages	Limitation
Bagya-lakshmi et al. [11]	Intrusion detection is supported by cyber analytics data mining techniques.	IDS are recycled to identify malicious action on the host as well as in the network.	Due to the massive amount of malicious data that DDoS attacks produce on the network, as one of the most difficult tasks in IDS
Almomani et al. [13]	ML approaches	innovative and creative solutions are required to improve IDS	Traffic get more sophisticated and difficult to identify as network traffic increases.
Bagaa et al. [14]	Revolutio-nary ML	Deals with the increasing security risks of the IoT automatically	There are many security risks that might impact the IoT, including Denial of Service (DoS) attacks, network invasions, along with data leaks.
SaiSindhu Theja et al. [15]	Crow Search Algorithm (CSA) as well as Opposition Based Learning (OBL)	Recurrent Neural Network (RNN) classifier is recycled for classification, along with Oppositional Crow Search Algorithm (OCSA) is cast-off	Attack detection framework is quite difficult
	technique	for feature selection.	
Tahir et al. [16]	CryptoGA,	To access services from any location in the world, CC is vital to the IT industry.	Many dangers and vulnerabilities are growing along with the popularity and demand for CC.

Table 1 details several novel techniques. Present methods include a plethora of proposed techniques, including Data mining, CryptoGA and CC.These technologies provide a advantages, including innovative and creative solutions are required to improve IDS.

Rabbani et al. [9] discussed to enhance cloud service providers' capacity to simulate user behavior. For the purpose of recognition as well as detection, a particle swarm optimization-based probabilistic NN (PSO-PNN). Using a multi-layer neural network, first categorized and identified the dangerous behaviors in the user behavior data after meaningfully altering it into a comprehensible format. The UNSW-NB15 dataset to characterize various forms of harmful behavior displayed by users in order to validate the proposed approach. Understanding the complete behavioral space of malware behavior allows for a significant improvement over conventional protection measures.

Gupta et al. [10] offered a unique paradigm that permits numerous users to safely exchange their data for different objectives, using probabilistic methods, ML, and encryption. The model outlines the communication protocol and access rules for the various untrusted parties processing the owners' data. The proposed methodology offers a strong mechanism for detection and prevention, hence reducing the danger of leakage. For the purposes of storage, analysis, along with data use, the organization's important data must be shared with numerous parties as well as stakeholders in a cloud environment. However, maintaining privacy while properly exchanging data with several parties has become one of the most difficult tasks in ensuring security.

Bagyalakshmi et al. [11] highlighted one popular and effective paradigm for organizing and providing services via the Internet is CC. In terms of data storage, it is changing the information technology landscape. Data security should be given top consideration when it comes to huge data storage requirements. A most significant security issues in the modern cyber environment is intrusion. Resources, data, and applications in a cloud environment are all susceptible to attack because of the networked structure of the cloud. In the cloud, IDS are used to identify malicious activity on the host and in the network. Due to the massive amount of malicious data that DDoS attacks produce on the network, as one of the most difficult tasks in IDS. Intrusion detection is supported by cyber analytics data mining techniques.

Thabit et al. [12] described some restrictions, though. CC security is increased using a novel style of cryptography that employs two layers of encryption. Based on Shannon's theory of confusion as well as diffusion, the first layer uses logical operations including shifting to split the original plaintext as well as key into equal halves, XOR along with XNOR, and. Cryptography , translation as well as transcription) are all natural processes that the second layer mimics, according to the Central Dogma of Molecular Biology. Genetic structures grounded in the Molecular

Biology Central Dogma serve as its inspiration. Encryption is the most crucial method for safeguarding data.

Almomani et al. [13] explained how assaults on traffic get more sophisticated and difficult to identify as network traffic increases. To categorize network risks, researchers have recently started experimenting with ML approaches in conjunction with CC technologies. As a result, this work need fresh ideas and original approaches to enhance IDS. Malicious Attack (MA) techniques have become more sophisticated over the years. This article tackles the root of the problem by noticing an intrusion in CC before it upsets normal network operations. MA technologies have evolved from traditional methods, including Probe, R2L, U2R MA along with DoS, particularly the zero-day attack in online mode.

Bagaa et al. [14] discussed to address the ever-increasing security risks posed by the Internet of Things and unveiled a groundbreaking ML security architecture. This solution utilizes the capabilities of Software Defined Networking (SDN) as well as Network Function Virtualization (NFV) to talk many security concerns. Both the reaction and monitoring agents in this AI framework use ML- models, which are divided into two categories: anomaly-based as well as network pattern analysis intrusion detection in IoT systems. The goals of the framework may be achieved via the use of neural networks, distributed data mining systems along with supervised learning. Academic and corporate communities are becoming interested in IoT security. There are a number of security risks that might impact IoT devices. These include denial-of-service attacks, breaches into networks, and data leaks.

SaiSindhuTheja et al. [15] described the nonlinear notion of interruption activities, peculiar system traffic behavior, and numerous variables in the problem space, the attack detection framework is quite difficult. In order to handle these kinds of problems, suggests an effective DoS attack detection system that makes use of the OCSA, which combines the CSA and OBL technique. The proposed method comprises of two stages: the RNN classifier is employed for classification, as well as OCSA is used for feature selection. The OCSA algorithm is used to pick the key characteristics, which are subsequently sent to the RNN classifier. During the testing phase that follows, the RNN classifier is used to classify incoming data.

Tahir et al. [16] applied on user demand, the cloud keeps services for software, infrastructure, as well as platform distribution across the Internet. Since it allows consumers to access services from any location in the globe, CC is vital to the IT industry. Many dangers and vulnerabilities are growing along with the popularity and demand for CC. The two most important concerns in CC are data integrity and privacy, which are important since the data is kept in several places. Therefore, the two main aspects of the CC environment that users are concerned about are data integrity and privacy protection safeguards. CryptoGA, based on a GA to address privacy and data integrity concerns.

III. PROPOSED METHODOLOGY

Figure 1 shows the proposed IDS framework. Gathering the required data for model creation is the first step. The NSL-KDD datasets were taken into account for this study. Feature Extraction (FE) as well as Data Processing (DP) comprise the second layer of the proposed architecture. At this stage, the dataset is normalised to guarantee accurate encoding of all categorical categories and normalisation of all numerical features. The dataset is cleaned and normalised before using the XGB algorithm. Based on an experimentally chosen FI threshold, this technique constructs a vector with the Feature Importance (FI) values along with selects the optimal feature subset. The process of creating models is the third architectural layer. Training, validation, and testing are the three main activities that take place simultaneously during this phase. The performance criteria are used to assess each of these phases. The optimal model selection for intrusion detection is the last stage [17].

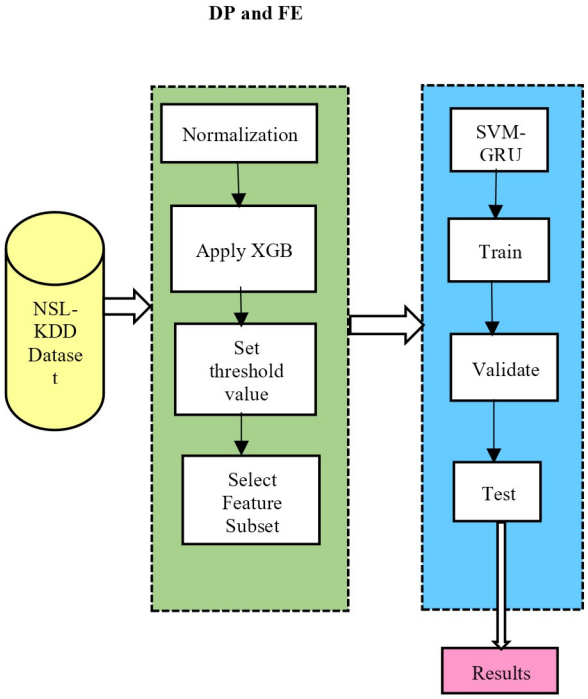

Fig. 1. An IDS based on RNNs

A. *Feature Normalization*

In the FE as well as DP phase of the proposed architecture, feature normalisation is a significant factor. This is because the majority of the characteristics in the datasets have values that do not fall neatly into a single range. Others are enormous, others are tiny, and some are even zeros. A large number of NNs (RNN types) were used in this investigation. Features with high values have the potential to degrade NN performance. Therefore, by decreasing the convergence rate during training, the normalisation method has been shown to improve NN performance. A dataset may be normalised in a variety of different ways, including decimal scaling, Min-Max scaling, Z-Score scaling, log normalisation, and more. More importantly, the application dictates the approach to be used. Nevertheless, this work opted for the Min-Max scaling strategy, as shown in Equation (1) for this investigation.

$$V_{norm} = \frac{V - V_{min}}{V_{max} - V_{min}} \quad (1)$$

Thus, by feature normalization the dataset features are normalized i.e. selected the features within a range.

B. *XGB feature selection*

The tree algorithm may be improved using the ML technique known as Extreme Gradient Boosting (XGB). This work produces the FI of each feature using XGB. Also, the XGB Classifier was used from the XGB Python package to try to do this. The technique also produces an optimal input vector that only contains features with the greatest FI relative to the FI threshold (FI_{th}). This number changes from dataset to dataset because it is chosen experimentally. The study's threshold value is a FI whose value is significantly lower than the following FI in the sequence. The following is the rule for selection of feature subset: When η is equal to 0.35, if $FI_{next} < \eta * FI_{current}$, then $FI_{th} = FI_{current}$ [17]. This condition is applied to the dataset to obtain the corresponding FI score.

C. *Classification*

To classify intrusions in the current system, researchers mostly employ ML algorithms along with data mining algorithms. The proposed DL algorithms to classify the intrusions, however, are the main focus of the proposed model. Several studies and investigations confirmed that DL algorithms outperformed ML and conventional algorithms in terms of accuracy. The RNN algorithm was covered in this study as a means to improve accuracy. See Figure 2 for a schematic of the proposed system's design.

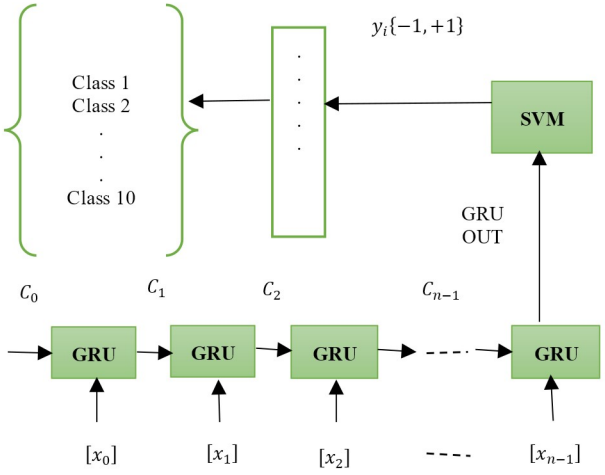

Fig. 2. The timestep, SVM classifier along with GRU input unit of the GRU-SVM model.

Integrate a SVM classifier into a GRU architecture. After that, the parameters are trained using the GRU architecture's gating mechanism . By including an RNN with update as well as reset gates that accept x_t and h_{t-1} as inputs and produce $\widehat{h_t}$, the GRU is able to circumvent the shortcomings of current RNNs.

Update gate Equation in (2):

$$z_t = \sigma(W_z.[Uh_{t-1}, x_t]) \quad (2)$$

Reset gate Equation in (3):

$$r_t = \sigma(W_r.[Uh_{t-1}, x_t]) \quad (3)$$

Candidate hidden state Equation in (4):

$$\widehat{h_t} = tanh(W.[r_t * h_{t-1}, x_t]) \quad (4)$$

Substituting the Leaky-ReLU (LRelu) activation function for the conventional hyperbolic tangent is the second adjustment. Specifically, this work adjusts the computation of the candidate state $\widehat{h_t}$ in Equation (5) in the following way:

$$\widehat{h_t} = LRelu(W.[r_t * h_{t-1}, x_t]) \quad (5)$$

Hidden state Equation in (6):

$$h_t = (1 - z_t) * h_{t-1} + z_t * \widehat{h_t} \quad (6)$$

where W and U denote weight matrices, σ denotes a logistic sigmoid activation function, as well as h_{t-1} represents the hidden state (derived from the previous time step t). The optimal separation hyper-plane parameters are resolved during the following regularisation by enhancing the main function of SVM, which is the last layer presented by SVM as well as its extra of the typical softmax layer in a GRU in Equation (7) and (8).

$$f(\widetilde{\omega}, \varepsilon) = min\frac{1}{2}\widetilde{\omega}^T w + C\sum_{i=1}^{N}\varepsilon_i \quad (7)$$

$$y_i\left(\widetilde{\omega}^T\varphi\left(\ddot{X}_t\right) + b\right) \geq 1 - \varepsilon_i and\ \varepsilon_i \geq 0, i = 1, \ldots N \quad (8)$$

Think about a collection of training data. The set G is defined as $G = \{[\ddot{x}_i, y_i]\}_{i=1}^{n}, \ddot{x}_i \epsilon R^m$. The input design i belongs to the set R^m and its corresponding observed outcome y_i, which might be anywhere from +1 to -1, is represented by bi. The test classification model uses y_i as the class label, where x_i is the characteristics of the text vector, and c is a constant that represents a compromise between the edge as well as the overall error computation. The input space is changed into a higher-dimensional feature space using the non-linear function $(\ddot{x})$. A 2/w margin separates the two halves. Preparation of the L2-SVM is necessary for the proposed GRU-SVM architecture. A score vector for each class is generated by the decision function $f(x) = sign(wx + b)$ when it comes to the prediction phase. Thus, the arrmax function is used to create the predict class label y from data x in Equation in (9):

$$predict - class = argmax\big(sign(wx + b)\big) \quad (9)$$

Here is a brief overview of the GRU-SVM method that has been proposed:

a. Then, feed the GRU network the dataset features $\{x_i | x_i \epsilon R^m\}$.

b. Then alter the learning parameters, weights and biases, throughout training. Start with arbitrary numbers.

c. The input characteristics x_i and the learning parameters of the GRU network cell are used to compute its state.

d. Using the SVM decision function: $f(x) = sign(wx + b)$, the model's prediction is calculated at the final time step.

e. Utilising an optimisation approach, namely the Adam optimizer, to minimise losses is the focus of this study. Using the calculated loss as a basis, optimisation modifies the biases and weights.

f. This is done again and again until the RNN has the right accuracy, or gets as accurate [18].

IV. RESULTS

The experimental procedures were executed using the ML and DL Python Libraries. Concerning the hardware system, all the simulations were run on a Windows 10 (OS) and a CPU with the following specifications: 1.80 GHz to 1.99 GHz, Processor: Intel(R)-Core(TM) i7-8568U.

A. NSL-KDD Dataset

An assessment that was deceptive and had a significant impact on the intrusion detection accuracy led to the development of the NSL-KDD dataset from the KDD Cup99 dataset. The massive volume of duplicate packets is particularly problematic in the KDD Cup99 dataset. Approximately 78% as well as 75% of the network packets are duplicates, of the KDD training along with test datasets. Due to the huge count of repeated instances in the training set, ML techniques would be biassed in favour of normal instances and would thus be unable to learn irregular cases, which are usually more harmful. In order to address these issues, the NSL-KDD dataset was created with the intention of removing duplicate entries. A total of 22,544 records make up the test dataset, whereas 125,973 records make up the NSL-KDD train dataset. Of the 41 characteristics, 22 are training intrusion attacks are selected. This selection is made by using the XGB feature selection algorithm using the FI score estimation. The attributes with the desired FI score are chosen for the classification process [19].

B. Performance metrics

A variety of performance measures are available for use in determining how effective is the proposed DL-based IDS system. A wide variety of measurement variables, including FPR, precision, detection rate (DR), F-measure, and accuracy (ACC), were used to display and assess the outcomes of the studies.

- True Positive (TP): The amount of MA cases properly classified as malicious;
- True Negative (TN): The amount of legitimate instance actions correctly classified as legitimate;
- False Positive (FP): The amount of legitimate instance events incorrectly classified as attack.
- False Negative (FN): The amount of MA occurrences that were incorrectly classified as legitimate operations [20].

By using these measures, the performance of this research is estimated and its mathematical formulation is depicted in Table 2.

TABLE II. MEASUREMENT FORMULA

Measurement	Formula
FNR	$FNR = \frac{FN}{(FN + TP)}$
FPR	$FDR = \frac{FP}{(TN + FP)}$
TPR	$DR = \frac{TP}{(TP + FN)}$
TNR	$TNR = \frac{TN}{(TN + FN)}$
ACC	$ACC = \frac{(TP + TN)}{(TP + TN + FP + FN)}$
Precision	$PREC = \frac{TP}{(TP + FP)}$
F-Measure	$F - measure = \frac{(2 \times Precision \times Recall)}{(Precision + Recall)}$

TABLE III. PERFORMANCE COMPARISON

Measurement	SVM	GRU	Proposed
FNR	0.117	0.105	0.0481
FPR	0.139	0.061	0.0190
TPR	0.858	0.947	0.9519
TNR	0.892	0.917	0.9810
ACC	0.858	0.946	0.9674
Precision	0.860	0.950	0.9775
F-Measure	0.858	0.947	0.9645

Various approaches' performance parameters are compared in Table 3. Compared to other models like SVM and GRU, the proposed model seems to perform better across all parameters. On the NSL-KDD dataset, the proposed model has an accuracy of about 96%. With a performance gap of 12.75 %, this model beats SVM and 2.26 % NN. Additionally, Figures 3 show the graph for these models. While working only with SVM and GRU since the models has some limitations there is still some issues with accurate detections. But since by using the hybrid model the limitations are removed and also provide an accurate results when compared to the existing approaches. As per the literature works discussed most limitations occur with efficient feature selection and accurate detection of attacks. This limitation is achieved in this proposed research.

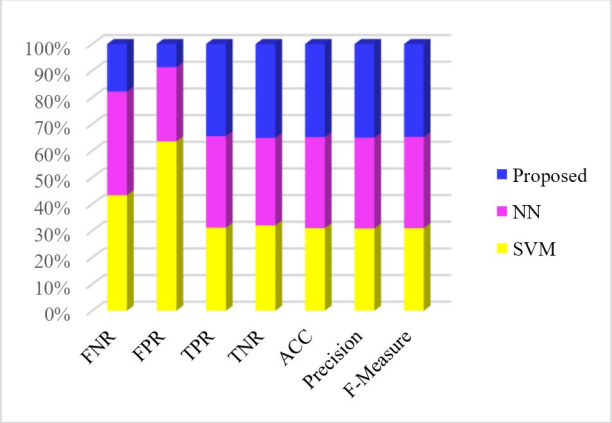

Fig. 3. Comparison graph with various measure

V. CONCLUSION

An IDS framework was described in this research that used a combination of the SVM-GRU approach and the XGB feature selection method. To evaluate the proposed classifier, the NSL-KDD dataset was used. By XGB feature selection the 41 features in the NSL-KDD dataset is reduced to 22 most significant features. This is achieved by using a condition called FI score detection. After feature selection the detection of attacks is done with aid of GRU-SVM approach. This approach achieved an accurate detection of attacks when compared to other works. According to the findings, the proposed approach was the most effective.

Since, wwhen compared to other methodologies, the results achieved by this framework were far better.

The future research goal is to expand the model's performance on minority classes and to examine how well the proposed framework performs on specific classes in the intrusion datasets. It will also put into practice a study of hybrid approaches, which are combinations of several RNN models.

REFERENCES

[1] Butt, Umer Ahmed, Muhammad Mehmood, Syed Bilal Hussain Shah, Rashid Amin, M. Waqas Shaukat, Syed Mohsan Raza, Doug Young Suh, and Md Jalil Piran. "A review of machine learning algorithms for cloud computing security." Electronics 9, no. 9 (2020): 1379.

[2] Nassif, Ali Bou, Manar Abu Talib, Qassim Nasir, Halah Albadani, and Fatima Mohamad Dakalbab. "Machine learning for cloud security: a systematic review." IEEE Access 9 (2021): 20717-20735.

[3] Stergiou, Christos L., Andreas P. Plageras, Konstantinos E. Psannis, and Brij B. Gupta. "Secure machine learning scenario from big data in cloud computing via internet of things network." Handbook of Computer Networks and Cyber Security: Principles and Paradigms (2020): 525-554.

[4] Bal, Prasanta Kumar, Sudhir Kumar Mohapatra, Tapan Kumar Das, Kathiravan Srinivasan, and Yuh-Chung Hu. "A joint resource allocation, security with efficient task scheduling in cloud computing using hybrid machine learning techniques." Sensors 22, no. 3 (2022): 1242.

[5] Kushwah, Gopal Singh, and Virender Ranga. "Optimized extreme learning machine for detecting DDoS attacks in cloud computing." Computers & Security 105 (2021): 102260.

[6] R. Senthilkumar, B. G. Geetha, "Asymmetric Key Blum-Goldwasser Cryptography for Cloud Services Communication Security," Journal of Internet Technology, vol. 21, no. 4 , pp. 929-939, Jul. 2020.

[7] Singh, Arun Pratap, Khel Prakash Jayant, Nidhi Bansal, Pratik Singh, and Amit Awasthi. "A proposal for advanced security system based on empirical technologies: cloud computing machine learning and the internet of things." Advances and Applications in Mathematical Sciences 20, no. 1 (2020): 175-190.

[8] Meryem, Amar, and Bouabid EL Ouahidi. "Hybrid intrusion detection system using machine learning." Network Security 2020, no. 5 (2020): 8-19.

[9] Rabbani, Mahdi, Yong Li Wang, Reza Khoshkangini, Hamed Jelodar, Ruxin Zhao, and Peng Hu. "A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing." Journal of Network and Computer Applications 151 (2020): 102507.

[10] Gupta, Ishu, Rishabh Gupta, Ashutosh Kumar Singh, and Rajkumar Buyya. "MLPAM: A machine learning and probabilistic analysis based model for preserving security and privacy in cloud environment." IEEE Systems Journal 15, no. 3 (2020): 4248-4259.

[11] Bagyalakshmi, C., and E. S. Samundeeswari. "DDoS attack classification on cloud environment using machine learning techniques with different feature selection methods." International Journal of Advanced Trends in Computer Science and Engineering 9, no. 5 (2020).

[12] Thabit, Fursan, Sharaf Alhomdy, and Sudhir Jagtap. "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions." International Journal of Intelligent Networks 2 (2021): 18-33.

[13] Almomani, Ammar, Mohammad Alauthman, Firas Albalas, O. Dorgham, and Atef Obeidat. "An online intrusion detection system to cloud computing based on NeuCube algorithms." In Cognitive Analytics: Concepts, Methodologies, Tools, and Applications, pp. 1042-1059. IGI global, 2020.

[14] Bagaa, Miloud, Tarik Taleb, Jorge Bernal Bernabe, and Antonio Skarmeta. "A machine learning security framework for iot systems." IEEE Access 8 (2020): 114066-114077.

[15] SaiSindhuTheja, Reddy, and Gopal K. Shyam. "An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment." Applied Soft Computing 100 (2021): 106997.

[16] Tahir, Muhammad, Muhammad Sardaraz, Zahid Mehmood, and Shakoor Muhammad. "CryptoGA: a cryptosystem based on genetic algorithm for cloud data security." Cluster Computing 24 (2021): 739-752.

[17] Senthil kumar, R., Geetha, B.G. Signature Verification and Bloom Hashing Technique for Efficient Cloud Data Storage. *Wireless Pers Commun* **103**, 3079–3097 (2018). https://doi.org/10.1007/s11277-018-5995-8

[18] Zulqarnain, Muhammad, Rozaida Ghazali, YM Mohmad Hassim, and Muhammad Rehan. "Text classification based on gated recurrent unit combines with support vector machine." International Journal of Electrical and Computer Engineering 10, no. 4 (2020): 3734-3742.

[19] Zhou, Shibo, and Xiaohua Li. "Spiking neural networks with single-spike temporal-coded neurons for network intrusion detection." In 2020 25th International Conference on Pattern Recognition (ICPR), pp. 8148-8155. IEEE, 2021.

[20] Almomani, Ammar, Mohammad Alauthman, Firas Albalas, O. Dorgham, and Atef Obeidat. "An online intrusion detection system to cloud computing based on NeuCube algorithms." In Cognitive Analytics: Concepts, Methodologies, Tools, and Applications, pp. 1042-1059. IGI global, 2020.