Optimized deep neural network based vulnerability detection enabled secured testing for cloud SaaS

Rohith Vallabhaneni[1], Sanjaikanth E. Vadakkethil Somanathan Pillai[2], Srinivas A. Vaddadi[1], Santosh Reddy Addula[1], Bhuvanesh Ananthan[3]
[1]Department of Information Technology, University of the Cumberlands, Williamsburg, USA
[2]School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks, USA
[3]Department of Electrical and Electronics Engineering, PSN College of Engineering and Technology, Tirunelveli, India

Article Info

Article history:

Received Mar 18, 2024
Revised Aug 19, 2024
Accepted Sep 2, 2024

Keywords:

Attack mitigation
Deep neural network
Features
Golf optimization algorithm
Vulnerability detection

ABSTRACT

Based on the information technology service model, an on-demand services towards user becomes cost effective, which is provided with cloud computing. The network attack is detected with research community that pays huge interest. The novel proposed framework is intended with the combination of mitigation and detection of attack. While enormous traffic is obtainable, extract the relevant fields decide with Software-as-a-service (SaaS) provider. According to the network vulnerability and mitigation procedure, perform deep learning-based attack detection model. The golf optimization algorithm (GOA) done the selection of features followed by deep neural network (DNN) detect the attacks from the selected features. The correntropy variational features validates the level of risk and performs vulnerability assessment. Perform the process of bait-oriented mitigation during the phase of attack mitigation. The proposed approach demonstrates 0.97kbps throughput with 0.2% packet loss ratio than traditional methods.

Corresponding Author:

Rohith Vallabhaneni
Department of Information Technology, University of the Cumberlands
Williamsburg, USA
Email: rohit.vallabhaneni.2222@gmail.com

1. INTRODUCTION

Through the web, consumers can link to and utilize applications that utilize the cloud thanks to Software-as-a-service (SaaS) [1]. Office supplies, organizing, and electronic communication are usual instances; it offers a whole package of applications that customers may obtain from an internet company on an hourly basis. Connectivity to computer systems, stored information, memory, and other capabilities is provided by a service; it enables businesses to buy assets as necessary, it is built on code that is freely available, referred to as open SaaS It is a software tool that runs on a website and is managed, endorsed, and managed by an internet service operator. Maintenance and new features are handled by the primary vendor, but the group of clients defines the development schedule for unified cloud-based software apps.

Many enterprises think that an internal cloud [2], offers more security for the sensitive information they store. But in actuality, cloud services have always been safer since the majority are managed by trustworthy individuals who are aware of potential risks and know how to address them. The safeguarding of information held on online servers against loss, alteration, and exploitation is known as cloud security [3]. Barriers, reconnaissance, deception, encoding, and preventing accessible internet links are some techniques used to provide online safety. The best cloud vendors include a combination of verification methods, encoding, distrust architectural designs, login and access control, and ongoing recording and tracking, in addition to secure-by-design facilities and multi-layer safety that are integrated into the software and its amenities.

This indicates that all of it is kept in safe locations, usually facilities. Cloud computing [4] includes secure documents, directories, and information, which makes it quite difficult for hackers to gain entry. These elements guarantee that the online archive is reliable and a secure location in which to keep important files. Additionally, it enhances creativity, enabling businesses to launch more quickly. Improved speed and effectiveness, greater adaptability and dependability, and a reduction in computer maintenance are all provided by the cloud. The listed drawbacks of cloud computation, such as rising safety and confidentiality concerns, an increase in hacking and uncontrolled possession of private data, continuous interruptions, restricted choices for modification, and a shortage of adaptability, can affect enterprises. This work proposed a novel optimized deep neural network (DNN) for detecting and mitigating the vulnerability in SaaS provider.

The remaining section of this research is arranged like; section 2 summarizes the literature reviews of existing works followed with the proposed framework is designed in section 3. After that, section 4 investigates the experimental results and the paper is concluded on section 5.

2. LITERATURE SURVEY

An attack detection-mitigation system has been presented incorporated with a framework of coordinated information safety, making use of a safe SaaS architecture [5]. When a malicious cluster is identified by deep belief network (DBN), power is passed to a minimal luring strategy that consistently neutralizes the majority of threat routers instead of interfering with regularly scheduled transactions. The protocol loss percentage and bandwidth were used to analyse how well the suggested tasks performed in comparison to the standard approaches. The suggested solution performs more efficiently than the remaining standard approaches, according to the findings. Hence, it is insufficient to interact with variable information sets.

ML modules enabling democratization and collaborating with commercial and academic groups to maximize the structure’s potential has been proposed [6]. Additionally, implementing decentralized and simultaneous instruction on various cluster configurations is being pursued as a means of improving performance. Enhancements to the retail sector are also anticipated, enabling sophisticated inquiries that make utilization of the component documentation to the fullest extent possible and advancing the content format. Therefore, it is inadequate to integrate storage in multiple locations.

Oppositional crow search algorithm (OCSA) has been proposed to handle enormous volumes of knowledge to secure SaaS [7]. The primary goal is to implement a novel, safe SaaS infrastructure by detecting attacks during periods of high traffic. A standard database is used to compare the performance of the suggested and traditional methods. Furthermore, with an effectiveness measure of 3% across all criteria, the suggested project outperforms the current operations. However, the ability to manage enormous volumes of information is lacking.

A hierarchical certificate-less aggregate signature to offer an internet-based SaaS verification mechanism that is flexible was presented [8]. Instead of confirming every client demand separately, the suggested remedy has the SC confirm the entire number of application instances to be issued from a consolidated connection demand. Under the dynamically selected signal threat, the suggested system remains reliable. The suggested approach effectively lowers the computational and interaction expenses associated with authenticating and validating cumulative connection requests, separately. Nevertheless, one particular point of lack arises during the client’s authentication process.

A Lyapunov-based decomposition strategy this divides the initial issue into three related separate issues was suggested [9]. It builds an internet resource decision and reliability control approach that resists intrusions and enhances the power balance by combining the approaches to address every one of the issues. Furthermore, dependability levels can be updated despite maintaining much historical data thanks to a compact reputation maintenance technique. But there is more difficulty in computation.

Feng and Liu [10] presented an overview of cloud resource scheduling solutions that employ deep reinforcement learning. These approaches reduce energy consumption while meeting significant demands for user services that are extremely dynamic, uncertain, and robust. Both surveys, however, do not provide a basic review of deep learning. Regarding applications, Khan *et al.* [11] provided an overview of mobile cloud architectures, cloud computing benefits, and mobile cloud offload decisions. The applications of mobile cloud computing (MCC) were covered, including mathematical tools, file search, photography tools, and gaming. Bera *et al.* [12] conducted an assessment of cloud computing applications in smart grids, notably in energy management, information management, and security. Cao *et al.* [13] conducted an assessment of cloud computing architectures that offer sensing, computation, control, and storage services for cyber-physical systems. Several applications, including smart grid development, intelligent transportation, tailored healthcare, and smart manufacturing, were examined. However, none of these survey publications focused on creating DNNs for cloud computing platforms. Soni and Kumar [14] and Khana *et al.* [15] provided overviews of machine learning technologies for a wide range of resource management activities, including workload estimation, task and virtual machine (VM) scheduling, resource optimization, and energy reduction. However, just a few deep learning (DL) technologies were briefly explored, and the previous DL surveys by Saiyeda and Mir [16] and Priya *et al.* [17] are either out of date or too brief. Many government [18], public [19], private [20], and commercial sectors [21] are becoming increasingly interested in creating cloud computing solutions for deep learning. Table 1 provides the research gaps and opportunities for future investigation.

Table 1. Research gaps and opportunities

Area	Research gaps	Opportunities
Scalability and performance	There might be insufficient focus on the scalability of optimized DNN models for large-scale SaaS environments, where applications are continuously evolving and generating vast amounts of data.	Investigate the scalability of DNN models and their ability to handle large datasets in real-time. Explore techniques such as distributed computing, parallel processing, and model optimization (e.g., pruning, quantization) to enhance performance and efficiency.
Adaptability to new vulnerabilities	DNN models may struggle to detect new and evolving vulnerabilities due to their reliance on historical data.	Implement adaptive learning mechanisms such as continual learning and few-shot learning to enable models to learn from new vulnerabilities as they emerge. Integrate anomaly detection methods to identify potential new threats that deviate from known patterns.
Model interpretability and explain ability	Deep learning models, including DNNs, are often considered black boxes, making it difficult to understand how decisions are made.	Enhance the interpretability and explainability of DNN-based vulnerability detection models. Utilize techniques such as SHAP (Shapley Additive explanations), LIME (Local interpretable model-agnostic explanations), and attention mechanisms to provide insights into the decision-making process, improving trust and adoption.

3. PROPOSED METHOD

The network vulnerability mitigation and attack detection development as the major intention of this work. Initially, the elliptical curve cryptography (ECC) obtains the gathered original information and performing data encryption with decryption. The feature selection performed with the usage of golf optimization algorithm (GOA) followed with the attack detection via DNN. Figure 1 depicts the overall workflow diagram.

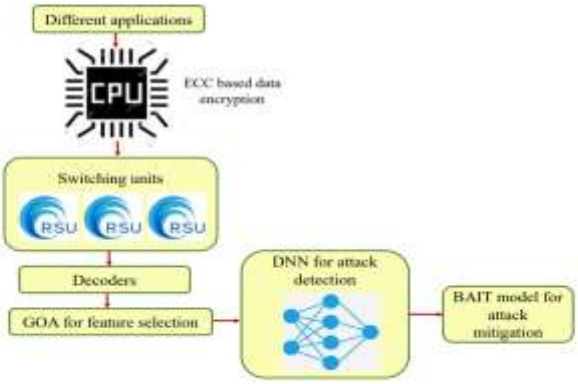
Different applications
CPU
ECC based data encryption
Switching units
RSU
RSU
RSU
Decoders
GOA for feature selection
DNN for attack detection
BAIT model for attack mitigation

Figure 1. Proposed workflow model

3.1. Data encryption

For public key system, apply and adopt elliptic curve cryptography (ECC), which has horizontal and vertical symmetry in Ellipse. The mathematical model of elliptic curve is expressed as (1),

$$z^2 = x^2 + cx + d \tag{1}$$

below expression writes the primes (P) with the finite filed (F_P) based on ECC [22].

$$z^2 = (x^3 + cx + d)\, mod\, P \tag{2}$$

The point doubling and addition are two major operations there by performing the operation of gradient η.

$$\eta = \frac{z_2 - z_1}{z_2 - z_1} mod\, \text{h}\, P \tag{3}$$

In the similar coordinates, both points to calculate the point doubling. The position beside the first coordinates is η with the lines passed to the result points.

$$\eta = \frac{3x_1^2 - c}{2z_1} \tag{4}$$

The upper bound of P with the private keys are δ_C and δ_D. This way obtains the each part of public key.

$$P_C = \delta_C H \tag{5}$$

$$P_D = \delta_D H \tag{6}$$

The following form encrypt the information towards cipher text with the usage of public key.

$$P_E = \{P_n + IP_D, IH\} \tag{7}$$

The user public key encrypt and change the message P_n. The cipher text results received from I as the random integer. The minor points with the operation of point addition against $P_n + IP_D$ is determined to perform data encryption. An authorized one access the message to encode the process as encryption and convert the data back into plaintext as the cipher text during decryption.

3.2. Selecting features

The GOA got its blueprint from the strategy of golf which is the outdoor game. The random search based appropriate solutions are taken for the initialized populations in the problem solving space [23]. For the selection features from the information we used this GOA in our work. The population is distributed uniformly and the locations are set randomly and the mathematical model is defined as,

$$Y = \begin{bmatrix} Y_1 \\ \vdots \\ Y_i \\ \vdots \\ Y_M \end{bmatrix}_{M \times N} = \begin{bmatrix} y_{1,1} & \cdots & y_{1,e} & \cdots & y_{1,N} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ y_{i,1} & \cdots & y_{i,e} & \cdots & y_{i,N} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ y_{M,1} & \cdots & y_{M,e} & \cdots & y_{M,N} \end{bmatrix}_{M \times N} \tag{8}$$

$$Y_i: y_{i,e} = LT_e + a \times (UT_e - LT_e) \tag{9}$$

Y is the GOA matrix population and the member is Y_i. The value of the eth function of the ith member as $y_{i,e}$. The random variable with the period of interval 0 and -1, members are M with the number of variables N. the upper and lower limits of eth variable are UT_e and LT_e. The mathematical illustration for the selection of features are stated in two phases, (i) exploration and exploitation and are described in the following section.

3.2.1. Exploration

The exploration ability of the GOA for selecting the features is enhanced with the following,

$$Y_i^{P1}: y_{i,e}^{P1} = y_{i,e} + a \times (H_e - I \times y_{i,e}) \tag{10}$$

$$Y_i = \begin{cases} Y_i^{P1}, G_i^{P1} < G_i \\ \quad Y_i, else \end{cases} \tag{11}$$

The new updated location of the features is Y_i^{P1} and the best member of the GOA is H with the objective function G_i^{P1}. The random number is I and lies in the range of 1 and 2.

3.2.2. Exploitation

In the exploitation stage the location updated using the objective function and the previously available data as shown,

$$Y_i^{P2}: y_{i,e}^{P2} = y_{i,e} + (1-2a) \times \frac{LT_e + a \times (UT_e - LT_e)}{t} \tag{12}$$

$$Y_i = \begin{cases} Y_i^{P2}, G_i^{P2} < G_i \\ \quad Y_i, else \end{cases} \tag{13}$$

the newly updated location in this state is Y_i^{P2} with the iteration count of t along the objective function G_i^{P2}. This process repeat till the best candidate solution attained for the feature selection.

3.3. Attack detection and vulnerability evaluation

To construct the DNN model for attack detection and to simulates similar hyper parameters with good accuracy. For each layer, the learning rate, batch size, cost function, activation function, number of nodes and layers are hyperparameters. The feed forward network is DNN to detect whether the attack is present or not [24]. Below function utilizes the input values in neural network.

$$\sum w_j q_j + a_j \tag{14}$$

The input value, weight and biased values arew_j, q_j and a_j. A hyperbolic tangent, rectifier threshold function and sigmoid are the activation function. In case of attack detection, we are using activation function as sigmoid in DNN.

$$\sigma(w) = 1/1 + e^{-w} \tag{15}$$

Compare the actual results with the attack detection output after fed the activation function of sigmoid. The loss function (LF) represented as the difference among the results,

$$LF = {}^{1}\!/_{2}\,(w_{HA} - w)^2 \tag{16}$$

achieve and minimize the loss function of network [25]. Figure 2 explains the DNN structure to detect attack.

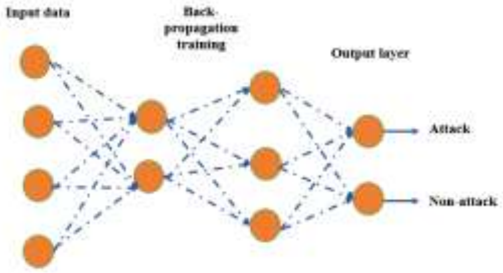

Figure 2. The DNN structure to detect attack

The DNN decides the defects is present or not. The network severity of risk level is predicted based on vulnerability assessment while the attacker presence is detected in the network. From DNN, normal and attack data is detected to validate the similarity among the attacked samples. Following formula computes the features of normal and attack of correntropy CE_χ.

$$CE_\chi(normal, attack) = F\left[K_\chi(attack - normal)\right] \tag{17}$$

The Gaussian kernel function is $F[\cdot]$ and χ is the size of kernel. The risk level is obtained with the normalized is the absolute variation.

$$Risklevel = \frac{\left| Cor^{\frac{Normal}{Examination}} - Cor_{Min}^{Normal} \right|}{Cor_{Mazx}^{Normal} - Cor_{Min}^{Normal}} \tag{18}$$

$$K_\delta(\cdot) = \frac{1}{\sqrt{2\pi\delta}} exp^{-\frac{(\cdot)}{2\delta^2}} h \tag{19}$$

$$\hat{U}_{N,\delta}(C,D) = \frac{1}{N} \sum_{j,k=1}^{N} \left[K_\delta \left(attack_j - normal_k \right) \right] \tag{20}$$

Where, Cor_{Mazx}^{Normal} and Cor_{Min}^{Normal} are the maximal and minimal correntropy over the normal samples. The mitigation attack approach transfer is controlled and higher risk level determines the anomalous samples. During data transfer, the normal routing is performed when the risk level is less than 0.5.

3.4. Attack mitigation

For attack node mitigation in system, this research utilized BAIT model, which involves route maintenance, attack node determination and mitigation with route discovery.

- Route determination: in the source node, the network obtains the packet of route request. Within cache routing tablet, the targets routing data is the neighbour source node. The information of route address towards PREQ packet is recorded with next hop nodes during the RPEQ route request prediction.
- Attack node detection and mitigation: for data transfer, transmit the data to best optimal node. While reaching the target, discards and attracts every data packets in this manner. The void routing table has PREP packet sent to these attacker nodes. The malicious node presence and absence PREP possibilities are checked during the suspicious reply reception. Verify the destination sequence number and parse the packet value in which the intermediate node receives the packet RPEP. The malicious nodes identifies the suspected node.
- Maintenance for route: from the errors, the network discard the malicious node. The shortest path is selected by selection as an essential. The ratio of packet delivery and throughput computes and accomplishes the shortest path identification.

4. RESULTS AND DISCUSSION

The experimental investigation of the proposed work is established in this section. This section employs, experimental setup along with comparative study with the existing works.

4.1. Experimental setup

For the experimental analysis we used the system with POSIX operating system incorporated with Intel Xenon Gold 6145 CPU, memory of 96 GB, in the platform framework of 64 bit ELF in a ROM of 16 GB. The simulation is effectuated in MATLAB 2019 a simulator. The experimental setup consisted of a high-performance, Unix-based environment with advanced CPU architecture, significant memory capacity, and a powerful simulation platform, ensuring robust and efficient performance during the simulation process.

4.2. Performance analysis of various parameters

For the analysis of the robustness of the proposed work in the secured cloud SaaS we have taken the statistical parameters such as encryption time, decryption time, accuracy, precision, pocket loss ratio, and throughput. The first two parameters are analysed with the existing cryptographic approach and rests of the parameters are analysed with the state-of-art work such as OCSA [7], ML [6], AT-MS [5], and LDS [9].

4.3. Encryption and decryption time

This is the predominant step in securing the data in the cloud SaaS, since the attackers can easily modifies the data. To overcome this, the proposed approach encrypts the data to the original source to identify whether it is attack or normal. For the comparison we have taken, the existing techniques such as reverse shamir adleman (RSA), quantum cryptography (QC), block ciphers (BC), and digital signatures (DS). Table 2 visualizes the tabular form of decryption and encryption time of proposed and other existing works. The Encryption and decryption time of proposed technique is lower with the time consumption of 85 ms and 58 ms respectively. Other works such as RSA, QC, BC, and DS consumes time of about 212 ms, 267 ms, 170 ms, and 145 ms respectively for encryption and for decryption 178 ms, 197 ms, 146 ms, and 128 ms correspondingly and are higher than the proposed technique.

Table 2. Performance analysis of proposed work based on the Encryption and decryption time with the state-of-art works

Techniques	Encryption time (ms)	Decryption Time (ms)
RSA	212	178
QC	267	197
BC	170	146
DS	145	128
Proposed	85	58

4.4. Accuracy and precision for the detection of attack

These parameters are taken to analyse the detection accuracy of the proposed work which implies the effectiveness. The visualization of accuracy of the attack detection is graphically illustrated in Figure 3. The plot is drawn better the parameters accuracy and learning percentage. The accuracy increases with the learning rate and for our proposed work when the learning rate is 90% the accuracy is 0.97 that is 97% which is higher than the existing approach while predicting the attacks. The other works such as OCSA, ML, AT-MS, and LDS achieved detection accuracies of around 0.8, 0.85, 0.83, and 0.9 respectively when the learning rate is equal to 90% as shown in Figure 3.

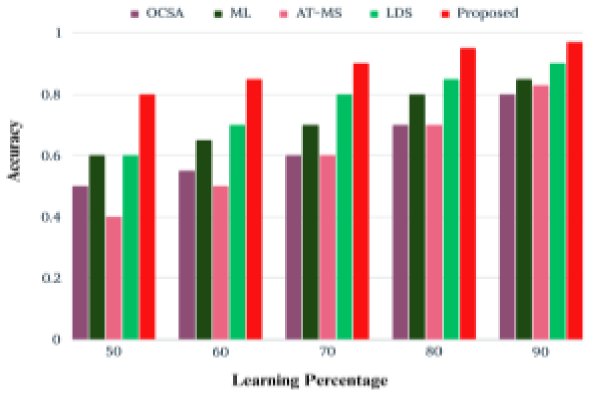

Figure 3. Visualization of accuracy vs. learning rate

The precision is another factor to evaluate the detection effectiveness of the proposed work and other existing works. Figure 4 illustrates the graphical representation of precision for the proposed work and existing works such as OCSA, ML, AT-MS, and LDS. The precision also plotted against the learning percentage and it elevated with the learning percentage increases. The precision of the proposed work is 0.96 that is 96% when the learning percentage is 90%. The other work achieves the precision rate at learning percentage 90% are 0.78, 0.8, 0.84, and 0.91 for the techniques OCSA, ML, AT-MS, and LDS correspondingly. This ensures the robustness of the proposed system over the other techniques.

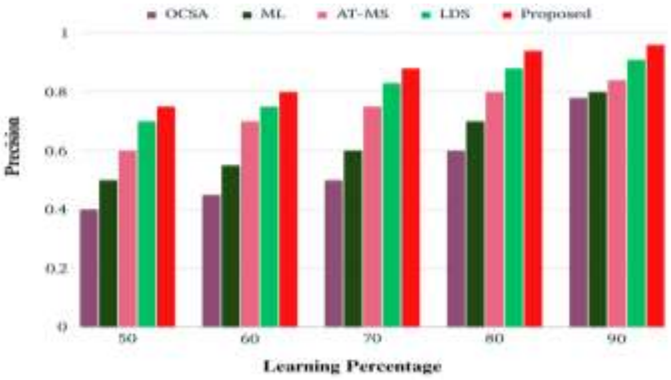

Figure 4. Visualization of precision vs. learning percentage

4.5. Packet loss ratio

Packet loss ratio is the important parameter for analysing the robustness of the proposed work while transmitting the information. If the cryptographic technique is effective then the proposed system will transform the information without any loss. Hence we analyse this parameter. The packet loss ratio against the attack rate is visualized in Figure 5. The packet loss ratio of the proposed work is lower 0.2 when the attack rate is 25. Meanwhile, the other techniques such as OCSA, ML, AT-MS, and LDS have higher packet loss ratio than the proposed as 0.9, 0.7, 0.8, and 0.6. Thus ensures the secured transmission in the cloud SaaS system.

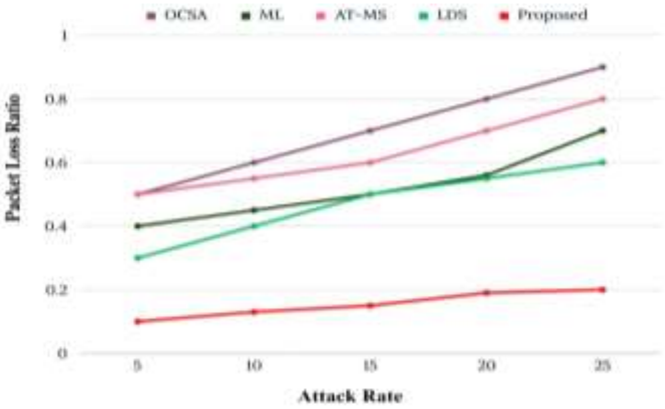

Figure 5. Packet loss ratio vs. attack rate

4.6. Throughput

This defines the delivery of the packets over the communication while performing the communication. It is analysed between the throughput and attack rate and plotted in Figure 6. Since the throughput mitigates with the attack rate, we analysed both the combination. The throughput of the proposed work is 0.78 when the attack rate is 25. Meanwhile, other approaches such as OCSA, ML, AT-MS, and LDS achieved the throughput of 0.3, 0.4, 0.3, and 0.7 when the attack rate is 25 respectively. The proposed work achieves higher throughput and ensures the robust communication.

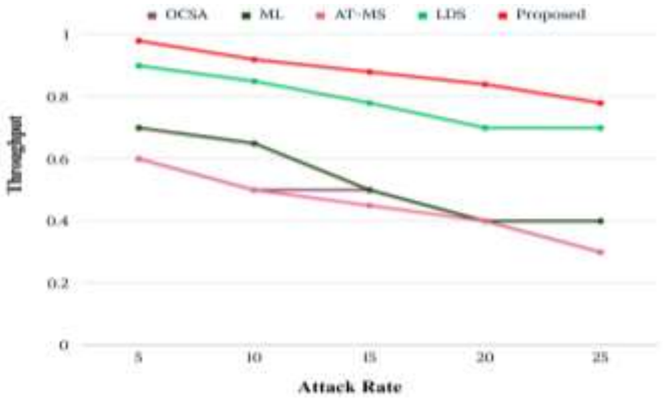

Figure 6. Throughput vs. attack rate

5. CONCLUSION

This section introduces the mitigation and attack detection. The mitigation process switch model and the network vulnerability and the deep learning model is performed the attack detection. The DNN model determines the attack in which the feature selection carried out via GOA. The features of correntropy variation risk level evaluation performs the assessment of vulnerability. The attack presence with network vulnerable is decided in this phase. The risk level threshold fixing based on the decision. Perform the mitigation process of BAIT during the phase of attack mitigation. The packet loss ratio validates the throughput, packet loss and accuracy. This section explores cloud migration and cross validation performed and real time cloud environment. The proposed approach demonstrates 0.97 kbps throughput with 0.2% packet loss ratio than traditional methods like OCSA, ML, AT-MS, and LDS.

ACKNOWLEDGEMENTS

The Author with a deep sense of gratitude would thank the supervisor for his guidance and constant support rendered during this research.

REFERENCES

[1] A. Bonadio, F. Chiti, and R. Fantacci, “Performance analysis of an edge computing SaaS system for mobile users,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2049-2057, 2019, doi: 10.1109/TVT.2019.2957938.

[2] C. Saju, P. A. Michael, and T. Jarin, “Modeling and control of a hybrid electric vehicle to optimize system performance for fuel efficiency,” *Sustainable Energy Technologies and Assessments*, vol. 52, pp. 102087, 2022, doi: 10.1016/j.seta.2022.102087.

[3] M. M. Ahsan, K. D. Gupta, A. K. Nag, S. Poudyal, A. Z. Kouzani, and M. P. Mahmud, “Applications and evaluations of bio-inspired approaches in cloud security: A review,” *IEEE Access*, vol. 8, pp. 180799-180814, 2020, doi: 10.1109/ACCESS.2020.3027841.

[4] M. Ulaganathan, R. Muniraj, T. Jarin, B. Deepanraj and C. Sreekanth, “Quasi Z Source Inverter Fed Induction Motor Drive Using Chaotic Carrier Sinusoidal PWM,” *2022 International Conference on Innovations in Science and Technology for Sustainable Development (ICISTSD),* Kollam, India, 2022, pp. 386-391, doi: 10.1109/ICISTSD55159.2022.10010557.

[5] S. Reddy, and G. K. Shyam, “A machine learning based attack detection and mitigation using a secure SaaS framework,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 7, pp. 4047-4061, 2022, doi: 10.1016/j.jksuci.2020.10.005.

[6] Á. L. García *et al.*, “A cloud-based framework for machine learning workloads and applications,” *IEEE Access*, vol. 8, pp. 18681-18692, 2020, doi: 10.1109/ACCESS.2020.2964386.

[7] R. Saisindhutheja and G. K. Shyam, “A hybridized machine learning model for optimal feature selection and attack detection in cloud SaaS framework,” *IoT and Analytics for Sensor Networks: Proceedings of ICWSNUCA 2021*, Springer Singapore, pp. 403-413, 2022, doi: 10.1007/978-981-16-2919-8_36.

[8] D. Tiwari and G. R. Gangadharan, “SecAuth-SaaS: a hierarchical certificateless aggregate signature for secure collaborative SaaS authentication in cloud computing,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 12, pp. 10539-10563, 2021, doi: 10.1007/s12652-020-02864-5.

[9] X. Zhu, Z. Di, Q. Yao, X. Dong, J. Wang, and Y. Shen, “Performance-power tradeoff in heterogeneous SaaS clouds with trustworthiness guarantee,” *IEEE Transactions on Computers*, 2022, doi: 10.1109/TC.2022.3214626.

[10] Y. Feng and F. Liu, “Resource management in cloud computing using deep reinforcement learning: a survey,” in *Procedings 10th Chinese Society of Aeronautics and Astronautics Youth Forum*, 2023, pp. 635–643.

[11] A. R. Khan, M. Othman, S. A. Madani, and S. U. Khan, “A survey of mobile cloud computing application models,” *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 393–413, 2014.

[12] S. Bera, S. Misra, and J. J. P. C. Rodrigues, “Cloud computing applications for smart grid: a survey,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1477–1494, May 2015.

[13] K. Cao, S. Y. Hu, Y. Shi, A. W. Colombo, S. Karnouskos, and X. Li, “A survey on edge and edge-cloud computing assisted cyber-physical systems,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7806–7819, Nov. 2021.

[14] D. Soni and N. Kumar, “Machine learning techniques in emerging cloud computing integrated paradigms: a survey and taxonomy,” *Journal of Network and Computer Applications*, vol. 205, 2022.

[15] T. Khana, W. H. Tiana, and R. Buyya, “Machine learning (ML)-centric resource management in cloud computing: a review and future directions,” *J. Netw. Comput. Appl.*, vol. 204, 2022.

[16] A. Saiyeda and M. A. Mir, “Cloud computing for deep learning analytics: A survey of current trends and challenges,” *International Journal of Advanced Research in Computer*, vol. 8, no. 2, 2017.

[17] P. S. Priya, P. Malik, A. Mehbodniya, V. Chaudhary, A. Sharma, and S. Ray, “The relationship between cloud computing and deep learning towards organizational commitment,” in *2nd International Conference on Innovative Practices in Technology and Management.*, 2022.

[18] F. Benedetto and A. Tedeschi, “Big data sentiment analysis for brand monitoring in social media streams by cloud computing,” in *Sentiment Analysis and Ontology Engineering*, Springer, 2016, pp. 341–377.

[19] S. Mohan, S. Mullapudi, S. Sammeta, P. Vijayvergia, and D. C. Anastasiu, “Stock price prediction using news sentiment analysis,” in *2019 IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService)*, IEEE, 2019, pp. 205–208.

[20] S. Prasomphan, “Improvement of chatbot in trading system for SMEs by using deep neural network,” in *2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, IEEE, 2019, pp. 517–522.

[21] D. Scheinert, A. Acker, L. Thamsen, M. K. Geldenhuys, and O. Kao, “Learning dependencies in distributed cloud applications to identify and localize anomalies,” in *IEEE/ACM International Workshop on Cloud Intelligence*, 2021, pp. 7–12.

[22] D. Natanael and D. Suryani, “Text encryption in android chat applications using elliptical curve cryptography (ECC),” *Procedia Computer Science*, vol. 135, pp. 283-291, 2018, doi: 10.1016/j.procs.2018.08.176.

[23] Z. Montazeri, T. Niknam, J. Aghaei, O. P. Malik, M. Dehghani, and G. Dhiman, “Golf optimization algorithm: a new game-based metaheuristic algorithm and its application to energy commitment problem considering resilience,” *Biomimetics*, vol. 8, no. 5, pp. 386, 2023, doi: 10.3390/biomimetics8050386.

[24] S. Naseer *et al.*, “Enhanced network anomaly detection based on deep neural networks,” *IEEE Access*, vol. 6, pp. 48231-48246, 2018, doi: 10.1109/access.2018.2863036.

[25] D. Erhan, C. Szegedy, A. Toshev, and D. Anguelov, “Scalable object detection using deep neural networks,” *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 2147-2154, 2014, doi: 10.1109/cvpr.2014.276.

BIOGRAPHIES OF AUTHORS

Dr. Rohith Vallabhaneni is a dedicated worker with a strong work ethic in leading teams to solve organizational issues. He is capable of learning all aspects of information within a company and using the technical knowledge and business background to effectively analyze security measures to determine their effectiveness in order to strengthen the overall security posture. He has great work ethic and outstanding team leadership skills and seek to accomplish organizational goals, while growing in knowledge and experience. He can be contacted at email: rohit.vallabhaneni.2222@gmail.com.

Sanjaikanth E. Vadakkethil Somanathan Pillai (senior member, IEEE) holds an M.S. in Software Engineering from The University of Texas at Austin, Texas, USA, and a B.E. from the University of Calicut, Kerala, India. Currently pursuing a Ph.D. in Computer Science at the University of North Dakota, Grand Forks, North Dakota, USA, his research spans diverse areas such as mobile networks, network security, privacy, location-based services, and misinformation detection. He is a proud member of Sigma Xi, The Scientific Research Honor Society, underlining his commitment to advancing scientific knowledge and research excellence. He can be contacted at email: s.evadakkethil@und.edu.

Srinivas A. Vaddadi is a dynamic and forward-thinking professional in the field of Cloud and DevSecOps. With a solid educational foundation in computer science, Srinivas embarked on a journey of continuous learning and professional growth. Their relentless pursuit of knowledge and commitment to staying at the forefront of industry advancements has earned them recognition as a thought leader in the cloud and DevSecOps space. He can be contacted at email: vsad93@gmail.com.

Santosh Reddy Addula a senior member of the IEEE, holds a Master of Science in Information Technology from the University of the Cumberlands in Kentucky, USA. With extensive experience in the IT industry, he has demonstrated expertise across multiple domains. Santosh is an innovator with a strong portfolio of patents and has significantly contributed to academic research through his articles as an author and co-author. Additionally, he serves as a reviewer for esteemed journals, reflecting his dedication to advancing knowledge and ensuring the quality of scholarly publications in his field. He can be contacted at email: santoshaddulait@gmail.com.

Dr. Bhuvanesh Ananthan received the B.E. degree in Electrical and Electronics Engineering from Anna University in 2012, M.Tech. in Power System Engineering from Kalasalingam University in 2014 and Ph.D. degree from Faculty of Electrical Engineering of Anna University in 2019. He has published more than 65 papers in reputed international journals, 25 papers in international conferences and 10 books. He is a life time member of International Society for Research and Development, International Association of Engineers. He can be contacted at email: bhuvanesh.ananthan@gmail.com.