IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 1, 2025

ETHEREAL WATCH: DEEP GENERATIVE VIGILANCE FOR CLOUD NETWOTK SECURITY

SaiPranaya Chepuri
Computer Science and Engineering(Cybersecurity)
Institute of Aeronautical Engineering
Dundigal, Hyderabad
21951A6244@iare.ac.in

Y.Manohar Reddy
Assistant Professor
Computer Science and Engineering (Cybersecurity)
Institute of Aeronautical Engineering
Dundigal, Hyderabad
y.manoharreddy@iare.ac.in

Dhasari Anusha
Computer Science and Engineering (Cybersecurity)
Institute of Aeronautical Engineering
Dundigal, Hyderabad
22955A6203@iare.ac.in

Rayavaram Saishatkari vija
Assistant Professor
Computer Science and Engineering(Cybersecurity)
Institute of Aeronautical Engineering
Dundigal, Hyderabad
22955a6205@iare.ac.in

Abstract: The undertaking's primary objective is to tackle the trouble of precisely recognizing unidentified attacks in the cloud climate by making and applying deep generative learning models that are uniquely intended for Cloud Intrusion Detection Systems (IDS). The recommended approach utilizes two particular deep generative models, the hybrid model CDAAE-KNN and the conditional denoising adversarial autoencoder (CDAAE), every one of which has an unmistakable capability in creating unsafe examples. To help grow the dataset for training the cloud IDS, explicit kinds of malevolent examples are created through the CDAAE. Pernicious marginal examples are delivered by the hybrid model CDAAE-KNN, and they are fundamental for working on the accuracy of the IDS by focusing on examples that are near the choice limit. The first dataset is joined with the destructive examples delivered by CDAAE and CDAAE-KNN to make improved datasets that contain a more extensive assortment of tests covering both specific noxious sorts and marginal circumstances. The enhanced datasets are utilized to prepare three ML calculations, and their presentation and viability in recognizing interruptions inside the cloud climate is evaluated. The goal of this stage is to completely analyze what the delivered tests mean for the precision and strength of the IDS. To work on the exactness and versatility of intrusion detection, the venture extends its capacities by coordinating a Stacking Classifier, which joins the Linear SVC with Logistic Regression and ExtraTree Classifier. With regards to spotting conceivable security gambles in cloud frameworks, this gathering technique performs better.

Keywords - Cloud systems, conditional denoising adversarial auto encoder, Kth Nearest Neighbour, deep learning, generative models, intrusion detection System (IDS).

1. INTRODUCTION

The most recent five years have seen outstanding development in the cloud computing business because of its monetary advantages. Worldwide distributed computing deals is $180B with 24% yearly increment [1]. Notwithstanding, broad distributed computing made cloud frameworks helpless against different cyberattacks. Hence, specialist co-ops and end clients are progressively worried about cloud security [2]. Intrusion detection systems (IDSs) are significant for distinguishing and impeding security dangers on cloud frameworks [3-6].

DDoS assault relief has been a concentration for IDS specialists as of late [7]. This is on the grounds that DDoS attacks are far and wide and harm cloud organizations' accessibility and notoriety. Two of the most unsafe DDoS attacks are low-rate and application layer or entryway level. These assaults by and large copy network examples to stow away. For example, DDoS low-rate attacks infuse low- volume genuine traffic gradually and utilize less PCs. These attacks have negligible traffic and may look bona fide,

consequently regular location devices might miss them [8]. Application layer attacks, a further developed type of DDoS assault, attempt to mirror client traffic, making them hard to distinguish. To veil their attacks, aggressors commonly use certifiable client demands. Most organization and application layer guards miss these dangers [9]. Furthermore, these assaults might be carried out using various application layer conventions, both association situated and connectionless, making them more dangerous.

Two techniques are utilized to distinguish destructive cloud activities: nonmachine learning and machine learning [10]. Nonmachine learning techniques [10] detect attacks utilizing cloud hurtful way of behaving. These methodologies are quick and precise in identifying past attacks. Their shortcoming is that they depend on assault marks and can't distinguish new attacks. In this manner, ML based methods have been made to address nonmachine learning frameworks' constraints.

Nonetheless, using ML to foster a dependable cloud IDS is troublesome. Reasons incorporate the quick advancement of refined cloud attacks. Absence of named noxious examples for ML models is another issue. Cloud conditions catch generally common traffic tests and a couple of interruptions. Accordingly, most cloud invasion datasets are slanted. The expectation model produced on slanted datasets utilizing average ML strategies might be one-sided and mistaken. ML calculations habitually decrease blunder to improve exactness. They disregard class dispersion/extent and class balance.

Gathering more unsafe examples might assist with obfuscating IDS datasets balance. Because of client protection and security issues, cloud frameworks make assault test assortment testing [11]. Cloud suppliers try not to reveal information that could compromise client security or framework honors. Consequently, slanted datasets are usually adjusted by resampling (oversampling and under inspecting) [12]. In any case, these techniques have restrictions. Under examining can lose significant data, however oversampling can deliver overfitting by arbitrarily reproducing minority class indistinguishable copies. Moreover, it doesn't address the "lack of data" issue.

2. LITERATURE REVIEW

Cloud reception is tormented by security issues. This prodded exploration and drives to address cloud security dangers. Alongside these security concerns, the cloud worldview presents extra viewpoints that empower new security strategies, procedures, and models. This exploration
[2] inspects the security advantages of utilizing various mists simultaneously. Security and protection abilities and conceivable outcomes are analyzed for different designs. IoT is a state of the art innovation that is changing lives. IoT's quick and expansive use makes the internet progressively helpless, particularly to IoT-put together attacks with respect to digital actual frameworks. Because of the billions of IoT gadgets, distinguishing and it is essential to shut down these attacks. Because of IoT gadgets' restricted energy and computational capacities and assailants' fast development, this try is troublesome. [3] Obscure IoT-based assaults are more disastrous since they might overpower most security arrangements and take more time to find and "fix". This study acquaints a portrayal learning approach with better expect and "depict" surprising attacks, empowering supervised learning-based anomaly detection. We make three regularized autoencoders (AEs) to gain a dormant portrayal from input information [13, 36, 37].

The bottleneck layers of these regularized AEs prepared supervisedly utilizing ordinary information and known IoT dangers will become arrangement calculation inputs. To test the models, we do far reaching probes nine current IoT datasets. Exploratory outcomes show that the new inert portrayal further develops supervised learning approaches for distinguishing obscure IoT dangers. We likewise do tests to decide what hyperparameters mean for the proposed models' exhibition. These models run in 1.3 ms, which is sensible. Programmers frequently execute various digital attacks [2] on CPS sensors to infiltrate it effectively. Recognizing various digital attacks has gotten little consideration. We address how to proficiently distinguish a few digital attacks on particular CPS sensors in this study [4]. We utilize random finite set (RFS) hypothesis and an iterative RFS-based Bayesian channel and its estimation to distinguish both the quantity of attacks and the attacked sensors. Four mathematical tests with various attacks show that the RFS-based strategy to CPS numerous attack detection works.

This study [5] utilizes a DNN to make an adaptable and powerful IDS to identify and order surprising cyberattacks. Static and dynamic strategies are expected to break down datasets made over the long run because of organization conduct change and assault advancement. This kind of investigation helps track down the ideal calculation for distinguishing future dangers. A total assessment of DNN and other customary ML classifier investigates public benchmark malware datasets is given. Hyperparameter determination procedures utilizing KDDCup 99 dataset [30, 31, 32] select ideal DNN boundaries and geographies [5]. All DNN preliminaries last 1,000 ages with a learning pace of 0.01-0.5. The DNN model that excelled on KDDCup 99 is benchmarked on NSL-KDD, UNSW-NB15, Kyoto, WSN-DS, and CICIDS 2017. Our DNN model passes IDS information into numerous secret layers to become familiar

with its theoretical and high-layered include portrayal. A complete exploratory test shows that DNNs beat standard ML classifiers. At last, we offer scale-half breed IDS- AlertNet, a profoundly versatile and mixture DNN system that can screen network traffic and host-level occasions continuously to detect cyberattacks.

The quick development of organization traffic has made stream based IDS handling modest quantities of traffic information significant. These frameworks additionally use anomaly-based ways to deal with distinguish obscure attacks. This study utilizes unsupervised deep learning and semi-supervised learning to detect uncommon organization traffic (or interruptions) utilizing stream based information [6]. Specifically, Autoencoder and Variational Autoencoder calculations recognized unseen attacks using stream properties. The investigations utilized stream based qualities accumulated from network traffic data, including customary and particular attacks. These methodologies were contrasted with One-Class Support Vector Machine for Receiver Operating Characteristics (ROC) and region under ROC bend [7, 9]. To assess strategy execution at various edge settings, ROC bends were investigated. In many trials, Variational Autoencoder outperforms Autoencoder and One-Class Support Vector Machine.

Wireless sensor networks (WSNs) are well known in IIoT settings because of their simplicity of arrangement. Due of reflexive bundle flooding DoS, WSNs are profoundly defenseless against security attacks. Assault recognition works with confirmation control and notoriety based procedures. Nonetheless, alleviating measures like blockage channel transmission for these attacks are as yet discussed [7]. WSNs' asset compelled hubs, like low transmission capacity, memory, and battery, make it hard to make effective methodology. A circulated clog control by means of obligation cycle limitation (D-ConCReCT) to recognize and moderate IIoT DoS is proposed. The significant point is to test its reasonableness in huge scope organizations and its capacity to cut discovery and alleviation times contrasted with unified clog the executives utilizing obligation cycle restriction. Our outcomes demonstrate the way that D- ConCReCT can relieve DoS assaults in a 500-hub sensor organization. and strength of intrusion detection, the undertaking grows its capacities by coordinating a Stacking Classifier, which joins the LinearSVC with Logistic Regression and Extratree Classifier. With regards to spotting conceivable security takes a chance in cloud frameworks, this gathering strategy performs better. An easy-to-understand Flask framework with SQLite network is proposed to upgrade client collaboration and testing. This ensures pragmatic ease of use in network protection applications by working with smooth register and signin tasks. The task's viability in handling security issues with cloud-based interruption recognition frameworks is credited to the combination of refined gathering methods with a natural UI.

ii) System Architecture:

The project architecture for "Deep Generative Learning Models for Cloud Intrusion Detection Systems" follows a systematic approach. It begins with the exploration and preprocessing of the dataset, crucial for effective model training. Training and testing sets are then created from the dataset, therefore providing the basis for model assessment. The core model, built for cloud intrusion detection, is extended with a Stacking Classifier incorporating SVM [28] for enhanced performance. The evaluation phase rigorously assesses the model's performance, considering key metrics. This comprehensive system architecture ensures a robust intrusion detection system tailored for cloud environments, with the ensemble model enhancing accuracy and adaptability to dynamic cyber threats, as validated through meticulous evaluation and analysis of its overall performance.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

3. METHODOLOGY

i) Proposed Work:

To further develop the training dataset for three ML calculations and produce extra vindictive examples, the task utilizes the deep generative models CDAAE and CDAAE- KNN [13, 17]. This works on the exactness of the cloud- based IDS, which is especially helpful in recognizing troublesome DDoS attacks [7, 9]. To work on the accuracy

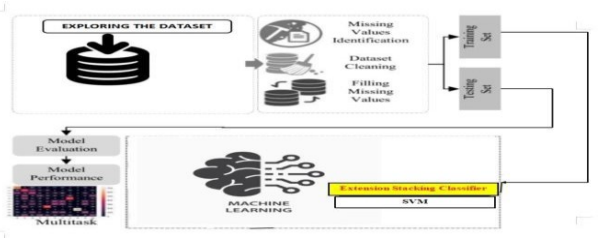

Fig 1: Proposed Architecture

iii) Dataset Collection:

This task involves looking into the utilized datasets. Compelling information readiness and afterward model training rely upon a consciousness of the design, attributes, and characteristics of the KDD CUP dataset and UNSW NB15 [43]. These datasets are utilized to show how well the proposed strategies identify attacks, accordingly demonstrating their proficiency.

'KDD CUP DATASET'

A well-known dataset for concentrating on IDS is KDD- CUP. The KDD-CUP dataset is utilized as a reason for training and surveying models with regards to deep generative learning models for cloud interruption discovery frameworks. This dataset might be utilized by profound generative models to remove complex examples and qualities from network traffic data, which will assist with making further developed IDS for cloud settings.

	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot
0	0	tcp	ftp_data	SF	491	0	0	0	0	0
1	0	udp	other	SF	146	0	0	0	0	0
2	0	tcp	private	S0	0	0	0	0	0	0
3	0	tcp	http	SF	232	8153	0	0	0	0
4	0	tcp	http	SF	199	420	0	0	0	0

5 rows × 42 columns

Fig 2: KDD CUP dataset

'UNSW-NB15 DATASET'

The UNSW-NB15 dataset is a modern network traffic dataset designed to address some limitations of earlier datasets like KDD-CUP. In the context of deep generative learning models, the UNSW-NB15 dataset is essential for enhancing intrusion detection capabilities in cloud environments. The dataset provides a more up-to-date and relevant set of network traffic data, which can be leveraged

	id	dur	proto	service	state	spkts	dpkts	sbytes	dbytes	rate	...
0	1	0.000011	udp	-	INT	2	0	496	0	90909.0902	...
1	2	0.000008	udp	-	INT	2	0	1762	0	125000.0003	...
2	3	0.000005	udp	-	INT	2	0	1068	0	200000.0051	...
3	4	0.000006	udp	-	INT	2	0	900	0	166666.6608	...
4	5	0.000010	udp	-	INT	2	0	2126	0	100000.0025	...

5 rows × 45 columns

ISSN 2347–3657
Volume 13, Issue 1, 2025

by deep generative learning models to extract intricate features and patterns to better detect intrusions and cyber threats in the cloud.

Fig 3: UNSW NB15 dataset

iv) Data Processing:

Data processing involves numerous fundamental cycles to prepared the dataset for productive intrusion detection. The first cloud intrusion detection dataset is first preprocessed by cleaning and normalizing the information to ensure consistency and limit inconsistencies. Consequently, the profound generative models, CDAAE and CDAAE-KNN, are utilized to deliver noxious examples. CDAAE produces designated unsafe information, though CDAAE-KNN makes marginal examples close to the choice limit, thus expanding the dataset's assortment. The made examples are incorporated into the first dataset, coming about in upgraded datasets. The improved information is exposed to feature extraction and scaling to guarantee interoperability with ML models. The handled datasets are eventually separated into preparing and testing sets, empowering the ML calculations to be educated, surveyed, and assessed for accuracy and execution in intrusion detection.

v) Feature selection:

Feature selection is significant for upgrading the adequacy of the IDS by knowing and safeguarding the most appropriate qualities from the dataset. The method involves assessing every trademark to discover its part in intrusion detection while killing copy or less significant components. Diminishing how much elements upgrades the framework's proficiency and speeds up training, subsequently working on the accuracy of ML models. This stage ensures that the intrusion detection models focus on the most basic components of the information to upgrade execution.

vi) Algorithms:

Random Forest, an ensemble method including many decision trees, improves detection by consolidating predictions from various trees. Its capacity to manage random subsets of data and attributes enhances resilience and precision, rendering it very effective for identifying intricate patterns within the enhanced intrusion detection dataset.

A **Decision Tree** systematically arranges judgments according to feature values in a flowchart format, classifying each sample by traversing a sequence of decision rules. Its interpretability and simple structure enable it to efficiently manage classification jobs for identifying intrusions in cloud settings.

Support Vector Machine (SVM) determines the best hyperplane that distinguishes several data classes, emphasizing the maximization of the margin between these classes. Its efficacy in high-dimensional regions renders it valuable for differentiating between normal and harmful behavior in cloud systems.

The Stacking Classifier integrates predictions from foundational models, such as ExtraTree Classifier and LinearSVC, into a superior Logistic Regression model. This method utilizes many viewpoints, improving the precision and resilience of the system in detecting security risks in the cloud environment.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

4. EXPERIMENTAL RESULTS

Precision: Precision measures among the ones categorized as positives the proportion of properly identified events or samples. The formula to determine the precision then is:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

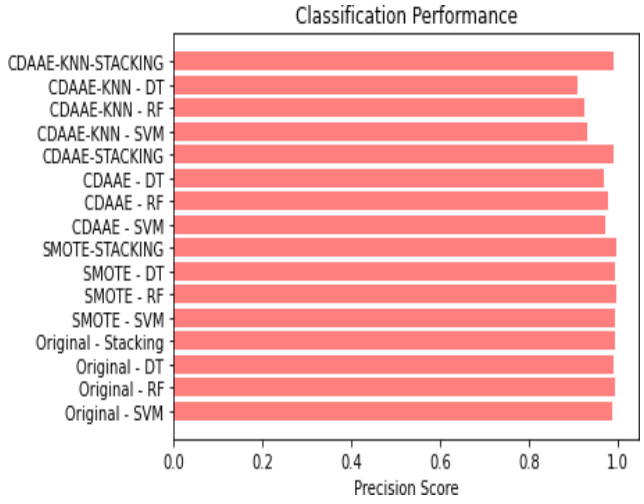

Fig 8: Precision Comparison Graph

Recall: In ML, recall is a statistic gauging a model's capacity to find all pertinent instances of a given class. It offers information on the completeness of a model in terms of accurately predicted positive observations to the overall actual positives.

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

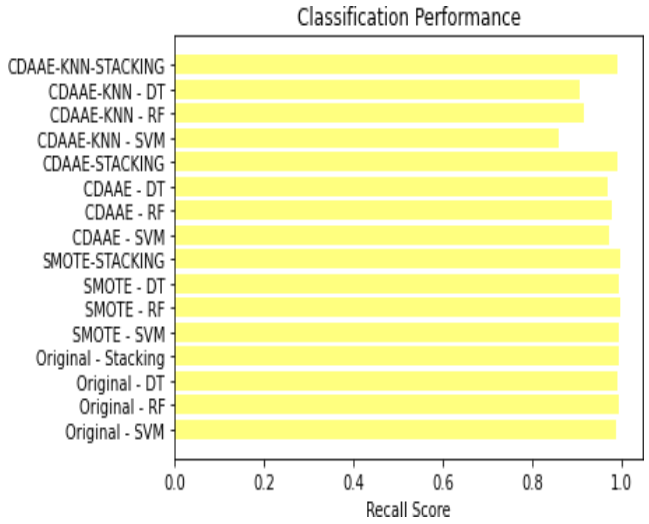

Fig 9: Recall comparison Graph

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

Accuracy: In a classification work, accuracy is the percentage of accurate predictions, thereby gauging the general performance of the predictions of a model.

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

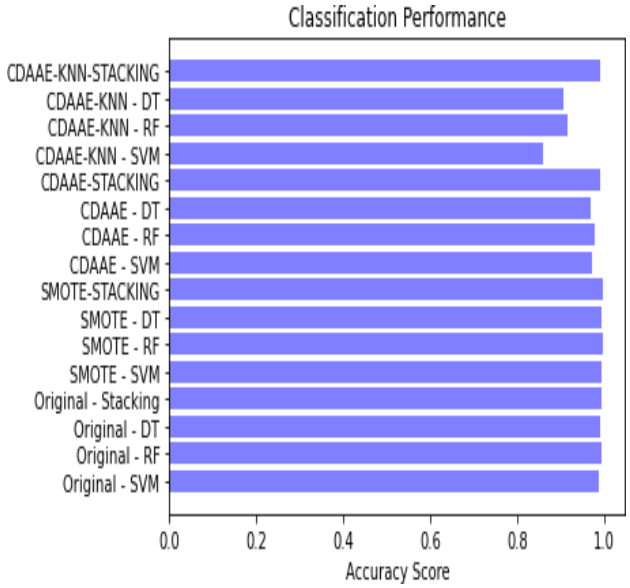

Fig 10: Accuracy Graph

F1 Score: The F1 score is suitable for imbalanced datasets and represents a balanced average of precision and hit rate, providing a balanced evaluation that includes both false positives and false negatives.

$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$

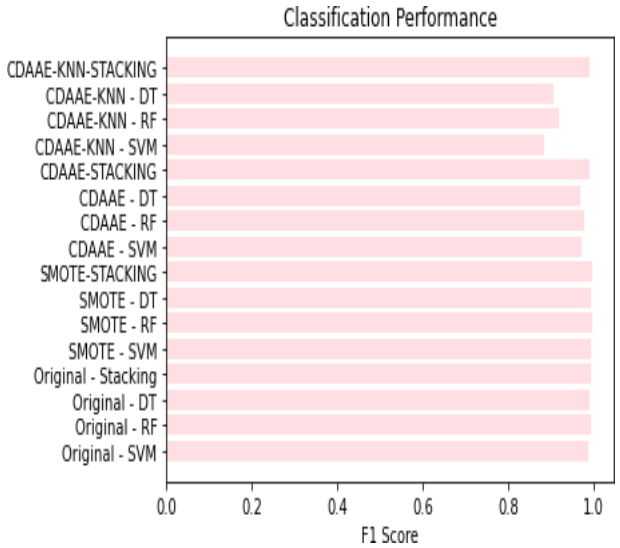

Fig 11: F1 Score

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

	ML Model	Accuracy	Precision	Recall	F1_score	AUC Score	Geometric Metric Score	Specificity	Sensitivity
0	Original - SVM	0.988	0.989	0.988	0.989	0.998	0.989	0.989	0.988
1	Original - RF	0.995	0.995	0.995	0.995	1.000	0.995	0.996	0.995
2	Original - DT	0.992	0.993	0.992	0.992	0.998	0.994	0.995	0.992
3	Original - Stacking	0.996	0.996	0.996	0.996	1.000	0.997	0.998	0.996
4	SMOTE - SVM	0.996	0.996	0.996	0.996	1.000	0.998	0.999	0.996
5	SMOTE - RF	0.999	0.999	0.999	0.999	1.000	1.000	1.000	0.999
6	SMOTE - DT	0.996	0.996	0.996	0.996	1.000	0.997	0.999	0.996
7	SMOTE-STACKING	0.998	0.998	0.998	0.998	1.000	0.999	1.000	0.998
8	CDAAE - SVM	0.972	0.973	0.972	0.972	0.997	0.974	0.976	0.972
9	CDAAE - RF	0.979	0.980	0.979	0.980	1.000	0.982	0.984	0.979
10	CDAAE - DT	0.969	0.971	0.969	0.970	0.964	0.972	0.975	0.969
11	CDAAE-STACKING	0.992	0.992	0.992	0.992	1.000	0.993	0.994	0.992
12	CDAAE-KNN - SVM	0.860	0.931	0.860	0.885	0.880	0.857	0.854	0.860
13	CDAAE-KNN - RF	0.917	0.926	0.917	0.920	1.000	0.924	0.930	0.917
14	CDAAE-KNN - DT	0.906	0.911	0.906	0.908	1.000	0.919	0.931	0.906
15	CDAAE-KNN-STACKING	0.992	0.992	0.992	0.992	1.000	0.993	0.994	0.992

Fig 12: Performance Evaluation

5. CONCLUSION

The CDAAE and CDAAE-KNN models are excellent methods for mitigating data imbalance in Intrusion Detection System (IDS) datasets [42] inside cloud settings. This is an essential measure for guaranteeing the precision and dependability of intrusion detection systems, especially in cloud settings susceptible to various cyber threats. These models, specifically, provide enhanced precision in identifying complex Distributed Denial of Service (DDoS) assaults, encompassing low-rate DDoS and application layer DDoS attacks [9, 19, 20]. Their effectiveness in identifying these sophisticated threats contributes to the overall robustness of the intrusion detection system, enhancing its capability to handle diverse and complex cyber threats. The project introduces ensemble techniques, such as the Stacking Classifier with Extratree Classifier + LinearSVC with LR, as an extension to the models. This ensemble approach demonstrates superior performance and robustness in intrusion detection. The diverse combination of classifiers within the ensemble enhances accuracy and adaptability, making it an effective solution for detecting intrusions in cloud environments. To enhance usability, the project incorporates a Flask-based user-friendly front end with secure authentication features. This ensures a practical and accessible solution for users interacting with the intrusion detection system. The integration of Flask and secure authentication adds a layer of robustness, making the system user-friendly while prioritizing data security, thus contributing to a comprehensive solution for intrusion detection in cloud environments.

6. FUTURE SCOPE

The future scope is to improve the accuracy and efficacy of cloud-based IDS using breakthroughs in deep generative learning models. This indicates a commitment to continuous improvement and refinement of the IDS for superior intrusion detection capabilities. Future efforts will focus on optimizing and fine-tuning the proposed models, CDAAE and CDAAE-KNN [13, 17]. This optimization will involve improving their ability to synthesize malicious samples, ultimately boosting the accuracy of the cloud IDS and making it more proficient in detecting a wide range of intrusions. The project envisions exploring additional deep learning techniques and algorithms beyond CDAAE and CDAAE-KNN. This exploration aims to broaden the horizons of the project by incorporating innovative methodologies to further enhance the detection and classification of unknown attacks within the cloud environment. The future scope emphasizes evaluating the proposed techniques on a larger

and more diverse set of IDS datasets [11]. This validation process is essential for assessing the effectiveness and generalizability of the developed methods, ensuring that the project's contributions are applicable across a broad spectrum of real-world intrusion scenarios.

REFERENCES

[1]. S.Natarajan, V.P. Vemuri, S.H. Krishna, Y. Manohar Reddy, P.Gundeshwar and S.Lakhanpal, "prediction Analysis of AI Adoption in Varioud Domain Using Random Forest Algorithm" 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), Gautam Budda Nagar, India, 2024, pp.1537-1541, doi: 10.1109/IC3SE62002.2024.10593362.

[2] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic minority over-sampling technique," J. Artif. Intell. Res., vol. 16, no. 1, pp. 321–357, 2002.

[3]. H. Han, W.-Y. Wang, and B.-H. Mao, "Borderline- SMOTE: A new oversampling method in imbalanced data sets learning," in Proc. Int. Conf. Intell. Comput., 2005,

pp. 878–887.

[4]. P. Vincent, H. Larochelle, Y. Bengio, and P.-A. Manzagol, "Extracting and composing robust features with denoising autoencoders," in Proc. 25th Int. Conf. Mach. Learn., 2008, pp. 1096–1103.

[5] X.-Y. Liu, J. Wu, and Z.-H. Zhou, "Exploratory undersampling for class-imbalance learning," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 39, no. 2, pp. 539–550,

Apr. 2009

[6] H. M. Nguyen, E. W. Cooper, and K. Kamei, "Borderline over-sampling for imbalanced data classification," Int. J. Knowl. Eng. Soft Data Paradigms, vol. 3, no. 1, pp. 4–21,

2011.

[7] D. Powers, "Evaluation: From precision, recall and F measure to ROC, informedness, markedness and correlation," J. Mach. Learn. Technol., vol. 2, no. 1, pp. 37– 63, 2011.

[8] D. P. Kingma and M. Welling, "Auto-encoding variational bayes," 2013, arXiv:1312.6114.

[9]. M. Bekkar, H. Djema, and T. Alitouche, "Evaluation measures for models assessment over imbalanced data sets,"

J. Inf. Eng. Appl., vol. 3, no. 10, pp. 27–38, 2013.

[10]. J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and

N. Marnau, "Security and privacy-enhancing multicloud architectures," IEEE Trans. Dependable Secure Comput., vol. 10, no. 4, pp. 212–224, Jul./Aug. 2013.

[11]. R. Longadge and S. Dongre, "Class imbalance problem in data mining review," 2013, arXiv:1305.1707.

[12]. I. Goodfellow et al., "Generative adversarial nets," in Advances in Neural Information Processing Systems, vol.

27. Red Hook, NY, USA: Curran Assoc., 2014, pp. 2672– 2680.

[13]. A. Makhzani, J. Shlens, N. Jaitly, I. Goodfellow, and B. Frey, "Adversarial autoencoders," 2015, arXiv:1511.05644. [14]. N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in Proc. Military Commun. Inf. Syst. Conf. (MilCIS), 2015, pp. 1–6.

[15]. B. Kiranmai and A. Damodaram, "Extenuate DDoS attacks in cloud," in Proc. 2nd Int. Conf. Appl. Theor.Comput. Commun. Technol. (iCATccT), 2016, pp. 235– 238.

[16]. R. Kumar, S. P. Lal, and A. Sharma, "Detecting denial of service attacks in the cloud," in Proc. IEEE 14th Int. Conf. Dependable Auton. Secure Comput. 14th Int. Conf. Pervasive Intell. Comput. 2nd Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech), 2016, pp. 309–

316.

ISSN 2347–3657
Volume 13, Issue 1, 2025

[17]. K. Wang and Y. Hou, "Detection method of SQL injection attack in cloud computing environment," in Proc. IEEE Adv. Inf. Manage. Commun. Electron. Autom. Control Conf. (IMCEC), 2016, pp. 487–493.

[18]. S. Wang, W. Liu, J. Wu, L. Cao, Q. Meng, and P. J. Kennedy, "Training deep neural networks on imbalanced data sets," in Proc. IEEE Int. Joint Conf. Neural Netw., 2016,
pp. 4368–4374.

[19]. T. Salimans, I. J. Goodfellow, W. Zaremba, V. Cheung,
A. Radford, and X. Chen, "Improved techniques for training GANs," in Proc. Annu. Conf. Neural Inf. Process. Syst., Barcelona, Spain, 2016, pp. 2226–2234.

[20]. A. D. Pozzolo, O. Caelen, S. Waterschoot, and G. Bontempi, "Racing for Unbalanced Methods Selection," in Proc. 14th Int. Conf. Intell. Data Eng. Autom. Learn., vol. 8206, 2013, pp. 24–31. Access, vol. 5, pp. 6036–6048, 2017.

[21]. P. Mishra, E. S. Pilli, V. Varadharajan, and U. K. Tupakula, "Intrusion detection techniques in cloud environment: A survey," J. Netw. Comput. Appl., vol. 77,
pp. 18–47, Jan. 2017.

[22]. J. Cervantes, F. García-Lamont, L. Rodríguez- Mazahua, A. López Chau, J. S. R. Castilla, and A. Trueba, "PSO-based method for SVM classification on skewed data sets," Neurocomputing, vol. 228, pp. 187–197, Mar. 2017. [23]. A. Karami, "An anomaly-based intrusion detection system in presence of benign outliers with visualization capabilities," Expert Syst. Appl., vol. 108, pp. 36–60, Oct. 2018.

[24]. K. K. Nguyen, D. T. Hoang, D. Niyato, P. Wang, D. N. Nguyen, and E. Dutkiewicz, "Cyberattack detection in mobile cloud computing: A deep learning approach," in Proc. IEEE Wireless Commun. Netw. Conf., 2018, pp. 1–6. [25]. S. H. Khan, M. Hayat, M. Bennamoun, F. A. Sohel, and R. Togneri, "Cost-sensitive learning of deep feature representations from imbalanced data," IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 8, pp. 3573–3587, Aug. 2018.

[26]. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proc. 4th Int. Conf. Inf. Syst. Security Privacy (ICISSP), Jan. 2018, pp. 1–9.