International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

AI-Driven Adaptive Intrusion Detection Framework for Cloud Environments Using Ensemble Learning and Behavioral Traffic Analytics

Mr. Sultan Saleem A[1], Aniruth A[2], Deepika B[3], Eazhlmahan ER[4], Hariprasath AS[5]

[1]Asst Professor, Dept of Computer Science & Engineering, Agni College of Technology, Chennai, India
[2,3,4,5]Student, Dept of Computer Science & Engineering, Agni College of Technology, Chennai, India

Abstract
The paper is an AI-based intrusion detection system (IDS) targeting a cloud computing system that is getting more vulnerable to more sophisticated cyber attacks, such as malware, denial-of-service attacks, and insider attacks that hinder the efficacy of conventional security systems in protection. The framework proposed combines machine learning based traffic analysis, behavioural modeling, ensemble learning, and adaptive retraining to detect not only known but also zero-day intrusions with a better set of reliability. Real time processing of network traffic, user activity patterns, and system logs are also done so that the IDS can identify abnormal deviations that are possible signs of malicious activities as well as minimize false alarms. Experiments on benchmark datasets and a MATLAB-type cloud infrastructure performance have proven good classification, steady behavior under detection, as well as being guarded against changing attack vectors. The continuous learning in the system is enhanced by the adaptive architecture which is appropriate in the dynamic cloud environment.

Keywords: Intrusion Detection System, Cloud Security, Machine Learning, Ensemble Learning, Behavioral Analytics, Zero-Day Detection, Cyber Threat Analysis.

INTRODUCTION

Cloud computing has changed the nature of deploying, controlling and scaling digital services by organizations in a way that is elastic, virtually a resource and accessible anywhere in the world. When businesses move important workload, sensitive information, and distributed applications to cloud infrastructure, a business becomes exposed to more cyberattacks in addition to generating a sophisticated security environment that cannot be fully effectively addressed by traditional security systems and systems. Multi-tenant architecture, shared responsibility model, and high interconnection of the clouds make them susceptible to attacks by intruders like DDoS attacks, spread of malware, misuse of credentials, and insider threats. Traditional security tools that are mainly based on fixed rules, moat signatures and manual controls is unable to check with new cyber attackers who continuously redesign operational strategies to avoid the security tracking systems [1]. This lapse is crucial in motivating intelligent,

dynamic, and scalable Intrusion Detection Systems (IDS) that incorporate machine learning and behavioral analytics to deliver real-time threat information.

The IDS structures driven by machine learning have crucial benefits over rule-based approaches because of the capacity to extrapolate patterns using data of the past, detect faint subtle anomalies in behavior, and also notice never-seen-before attacks. Within the clouds world, enormous volumes of heterogeneous data are created, which comprise network flows, system logs, user access and activity records. Conventional IDS technologies do not have the power to handle this high-volume, high-speed data stream in real-time, and thus they detect very slowly and yield a higher number of false positives. AI-driven methods use classification, clustering, and ensemble learning to dynamically read intricate patterns to give stronger detection of zero-day threats [2]. In addition, behavioral analytics can develop better insights into user and workload profiles enabling the system to recognize variations that could be a sign of insider attacks or covert reconnaissance patterns.

The introduction of rich benchmarking data including NSL-KDD and CIC-IDS2017 has been feasible in the training and testing of machine-learning-based IDS models. These datasets offer varied classes of attack, natural traffic patterns and constrained examination conditions that assist researchers in developing models that can manage real-world issues. In combination with simulated environments and managed cloud systems, these datasets can be used to carry out a systematic experiment, cross-validation, and performance benchmarking [3]. Also, expansion of cloud-based, simulation software, such as MATLAB, facilitates in-depth modeling of network behavior, load balancing and interactions between virtual machines, whereby researchers can examine the responsiveness of the system to different attack levels.

Latest research findings point out that intrusion detection in cloud configurations cannot be based on one algorithmic technique. The methods of ensemble learning, including random forests, boosted trees, and hybrid neural networks, provide much better results as they combine several classifiers into an improved performance in robustness, accuracy and generalization. The ensemble-based IDS models alleviate the classification bias, better scale to the high-dimensional data, and respond more to the dynamism of cloud traffic. These methods can be supported by adaptive retraining mechanisms so that the IDS can be kept abreast with changes in the threats posed by the new attacks, enhancing its reliability over a long period [4]. In addition, active monitoring activities of the systems can help identify slow-moving or low frequency attacks - a situation that would be vastly ignored by the traditional detection systems since it has limited temporal awareness.

Cloud distributed workloads require the IDS solutions to have minimal performance overheads because too much computing can result into poor quality of services. The scaling of the IDS components is required to be horizontal, and the detection time should remain fast as the infrastructure gains expansion at distributed data centers and on the virtualized nodes. This requirement can be met by real-time analytics engines, streaming classifiers, and feature-efficient detection algorithms that handle traffic patterns with lowbinary. Moreover, incorporation of threat intelligence feeds and situational intelligence facilitates collaborative security infrastructure with the ability to correlate events within distributed cloud systems. These capabilities are essential in detecting multi-vector attacks which entails simultaneous attacks on many endpoints [5]. So the architectural design of an AI-controlled IDS should be based on those attributes that should be; scalable, flexible, and efficient in computation.

The other key issue of cloud IDS research is the problem of imbalanced data. Encountering normal data dominance in real-world settings and infrequent intrusion, usually of a zero-day attack, in datasets are the norm. Machine learning algorithms can be preferential to normal classes providing less detection power

to rare, but important types of attacks. Oversampling, undersampling, feature optimization and cost-sensitive learning are some of the methods used to alleviate this problem and enhance the performance of the classifier. Moreover, modeling-based anomaly detectors can detect new attacks by indicating anomalies even when little training data marked as legitimate exists. This feature is especially significant in the cloud environments where attackers often change payload structures, communication patterns, and evasion methods.

Moreover, the combination of behavioral analytics and the traffic analysis enhances the ability of the IDS to detect the threat of an insider- one of the most challenging types of attacks in terms of detection. Insiders will either have valid access privileges and signature-based methods will be useless. However, behavioral models trace the user activity patterns, resource interactions, and workflow habits. In the case of deviations, e.g., when there are abnormal file transfers, abnormal login times, abnormal virtual machine interactions or abnormal command executions, the IDS can detect suspicious behavior without having predefined attack signatures. This preemptive monitoring improves the general security posture of the clouds.

LITERATURE SURVEY

The swift expansion of interlinked digital ecosystems has greatly expanded the attack area of the contemporary networks, necessitating smarter and flexible detection of intrusion. Conventional rule-based systems, which are quite effective when applied to known threats, have problems managing highly dynamic and evolving cyberattacks. With the larger adoption of IoT, IIoT, IoMT, and cyber-physical infrastructures into organizations, the amount, speed and diversity of data being generated is increasing exponentially to the point that scalable intrusion detection solutions are suddenly in demand to handle large scale heterogeneous data on demand. Machine learning (ML), deep learning (DL) and hybrid intelligence models have become the potent tools of the increased detection accuracy, fully automatic feature detection, and robustness of the system. Such developments have facilitated the use of network-based and host-based intrusion detection systems into adaptive models in responding to anomalies in various environments. It is against this background that researchers have explored a lot of schemes to enhance the performance of detection, optimisation on computational efficiency and the architectures which seamlessly merge with modern distributed infrastructures.

The recent research indicates the significant role of anomaly detection, dataset generation, and benchmarking for enhancing the intrusion detection performance. An example can be given such as anomaly-based detection models of medical IoT Networks proposed in [6] proving that the integration of several ML algorithms and customized set of data can enhance in identifying abnormal behavior in resource limited IoMT networks. The perspectives on the gap between AI/ML studies and the use in practice include a comprehensive approach to the problem of bridging research and practical considerations of the usability, privacy, and real-world applications, as proposed in [7]. Also, the optimization approaches represented by big data, as addressed in [8], suggest that the successful feature extraction and learning sample modelling help improve the overall detection success by a significant margin. Host-based intrusion detection systems (HIDSs) have also received a wide literature review, and a systematic review of developments in machine learning and deep learning-oriented HIDS architectures is provided in [9], and hybridized IIoT IDPS solutions in [10] are shown to improve the integrity and resilience of industrial systems through the combination of ML, DL, and blockchain components. Moreover, specific issues arising in the sector (as in drone path maintenance) are considered in [11], in

which systematic reviews are performed on the evaluation of lightweight anomaly detection mechanisms depending on autonomous airstrikes.

The domain-specific intrusion detection system has also received attention by the researchers based on optimizing features and employing sophisticated deep learning models. The models analyzed in [12] of smart grid intrusion detection demonstrate that better feature selection techniques, especially those based on gravitational search algorithms, can be rather helpful in improving the classification in critical power infrastructures. The application of host-based intrusion detection to the realm of IoT is discussed in [13] and the significance of privacy-sensitive and AI-driven classification algorithms. In the meantime, a dynamic generative AI-based architecture, such as the one proposed in [14], is employed to tackle automotive security problems, as it is an upgraded system to identify vehicles intrusion through VAE-based encoding and dynamic learning. The specialized detection architectures are also relevant to SCADA systems, the core of the power grid functioning, as the better LSTM- and FNN-based algorithm in [15] demonstrates the increased abilities of identifications of anomalies and their further response in industrial control environments. Increasing need of high-quality datasets is one of the points in [16] where a single multimodal dataset is suggested to enhance benchmarking stability and the possibility to train more robust models of intrusion detection under a heterogeneous network.

Lightweight, hierarchical and hybrid deep learning techniques are also vital to the progress of intrusion detection research in different network settings. Hierarchical classification models that are explained in [17] in which the weights are lightweight can be applied to improve an equalization of detection efficiency and can thus be deployed in delay-sensitive or resource-limited models. Equally, hybrid deep learning entails the integration of both spatial and temporal characteristic models, e.g., the EESNN model in [18] applies GAN-based data-enhancement, attention-based mechanism using transformers, and feature-based convolution to detect intrusion patterns at a high level. The hybrid IDS set up offered in [19] can benefit small and medium enterprises that are usually resource constrained since it offers a scaling threat monitoring and a scalable alert-scoring system that is adapted to the realistic business setting. Also, zero-touch network security solutions using deep learning like the one suggested in [20], provide automatic protection measures developed to apply to autonomous networks and smart city infrastructure, where real-time protection and limited human factors are critical.

METHODOLOGY

The design of the methodology of the proposed AI-driven Intrusion Detection System (IDS) is designed so that it provides the system to handle data systematically, design the models, perform the evaluation of the performance, and allow the adaptation of the system. The method combines machine learning, ensemble classifier, behavioral analytics, and real-time monitoring features to develop a powerful IDS that could be used in cloud systems. The stages are implemented to support scalability, accuracy, and resilience to the changing cyber threats. Its methodology starts with dataset preparation, moves onto feature engineering, model building, ensemble integration, adaptive retraining and real-time deployment. It is this systematic procedure that guarantees that the IDS is capable of quickly identifying known and unknown intrusions by the virtue of life-long learning as well as dynamic pattern identification. The subsections given below describe each methodological stage step-wisely and technically without the use of bullets or subheadings as shown in figure 1.

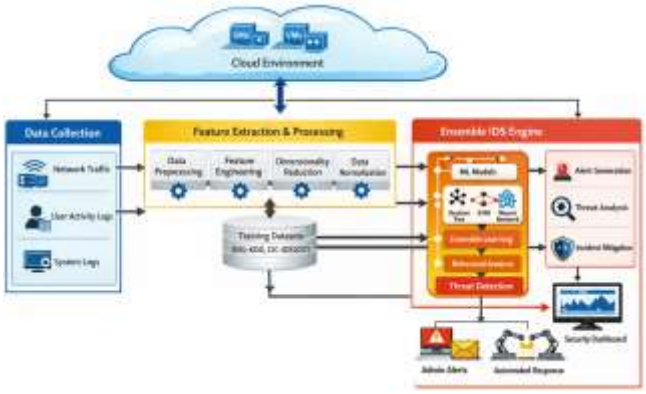

Fig. 1: System Architecture

A. Dataset Raising and Preprocessing.

This step is aimed at acquiring quality intrusion detection data, as well as at readying them to undergo machine learning processes. The benchmark datasets like either NSL-KDD or CIC-IDS2017 are loaded to reflect the variety of attack types, normal traffic patterns, and customary cloud-network patterns. The crude records are then cleansed to deal with missing entries, inconsistent labels and inaccurate traffic patterns that are likely to give rise to misleading model performance. Traffic flows and log samples are normalized in order to have homogenous scaling of all attributes. To remove bias in the classifier, duplicate entries are filtered off and to facilitate machine-learning algorithms, the categorical features are coded. Another preprocess that is carried is balanced data set where oversampling or controlled undersampling is applied in order to balance the uneven distribution of the classes. The processed and standardized data makes sure that further steps of training models use clean high-quality data that is statistically representative.

B. Dimensionality Optimization and Feature Engineering.

Feature engineering is carried out to derive significant features to the network traffic and log data and minimizes computational costs. Statistical and temporal features are also compromised with content-based features in evaluating their significance in detecting malicious traffic patterns. The techniques applied to high-dimensional sets of features include correlation filtering, recursive elimination and principal component analysis. These techniques lower noise, decrease redundancy and increase the explainability of the classifier. Behavior patterns are also added such as frequency of user accesses, and anomalies on sessions to enhance the ability of the system to identify insiders threats and zero-day attacks. Normalization makes the numeric attributes to have similar influence when learning. The optimized feature vector increases model stability by enabling the algorithms to work on the most discriminative attribute and this enhances the prediction and reduces the false alarms.

C. Machine Learning Model Construction.

The step entails training of individual machine-learning classifiers which are the basic building blocks of the IDS. Decision trees, support vector machines, deep neural networks and k-nearest neighbors, are some of the algorithms to be trained in order to identify a wide range of attack signatures and abnormal activity. All classifiers are trained in cycles which are usually followed with cross-validation so that they are not over-fitted and that their generalization capabilities are independent. Hyperparameters are optimized in such a manner that the best configuration is found in both speed and accuracy. The models are trained to learn the intricate associations between features and the attack classes during training so that they are able to differentiate between benign and malicious traffic within clouds. The individual models offer a variety

of analytical orientation that are subsequently aggregated in the ensemble phase which guarantees the provision of more intrusion detecting capabilities.

D. Learning Activities: Integration with Ensemble Learning.

The ensemble integration brings together the the power of the individual classifiers in a single detection engine. Stacking, boosting, and weighted voting are techniques used to combine decision tree, neural network and support vector machine output. The ensemble performs the role of lowering classification variance, rising to sturdiness to noisy samples, and improving the accuracy of several categories of attacks. Weighted methods guarantee that the most productive classifiers would have greater input to the final decisions. The last ensemble model is confirmed with the strategies of cross-fold in order to be consistent across unknown data. This brings with it a better ability to generalize and an increase in exposure to low-frequency attacks which are frequently not picked up by single models. The orchestra is the main analytical processing unit of the AI-based IDS.

E. update cycle of Adaptive Retraining and Model Update.

Intelligent retraining makes sure that the IDS is successful in evolving in response to changing cyber threat by regularly updated model parameters. A dynamic learning repository is a storage that stores real-time traffic feedback and anomalies that may have been identified. These samples are periodically added to incremental training steps that update the ensemble model without necessarily retraining it. This dynamic approach enables the IDS to acquire new attack patterns, changes in user actions, and new deviations of traffic. Drift-detection mechanisms observe any change in data distribution and therefore can issue retraining events when required. The update cycle enhances the long-term stability of the model, retards the decrease in the accuracy, and secures resistance to zero-day threats. The IDS is able to grow along with the cloud environment through adaptive learning.

F. Architecture of Real Time Deployment and Alerting.

The last phase deploys the IDS on a simulated cloud environment to assist in the real-time intrusion detection. Network packets, user sessions and system logs are all monitored by the data collectors and fed into the feature extraction pipeline and ensemble classifier. The system monitors the traffic in real time and sends alerts in case of anomalies or attack signatures. An alert-to-context mapping of alerts and contextual metadata is done by a decision-support layer to eliminate the number of false positives and to offer valuable security information. The architecture is also designed in such a way that the latency is minimized, detection activities will not affect the cloud performance. The administrators see the alerts in the form of dashboards and can quickly respond to such attacks and prevent them. This deployment architecture enables easy attachment to distributed clouds infrastructures and provides high rate of detection.

RESULT AND DISCUSSION

It appraises the efficacy, consistency, and scalability of the suggested AI-based Intrusion Detection System (IDS) in benchmark datasets in cloud simulated MATLAB contexts. The system was subjected to the load of different traffic in it, different types of attacks, and dynamics in the behavior of the system so as to ascertain the correctness of its detection and the system as a whole. The analysis is based on the accuracy of classification, computational efficiency, the ability to reduce false positives, cross-validation consistency, and response to new threats. This section shows the strengths and limitations of the IDS through performance analysis in different scenarios of the experiment and also shows its practical suitability in real cloud infrastructures. The results can be seen in both the quantitative measures of results

of the structured experiments and qualitative measures of results based on the behavioral patterns, algorithmic reactions, and interactions of the ensemble models.

Early experiments were performed with NSL-KDD and CIC-IDS2017 data to study the general capability of detection with regard to common types of attacks. The IDS was found to be highly accurate in its differentiation of normal and malicious traffic on a consistent basis which was greatly enhanced by the optimization of features as well as an ensemble. In preliminary experiments, single classifiers like decision trees and SVMs that yielded comparatively good accuracy had the disadvantage of misclassification in some cases in attack classes in the minority. Neural networks were superior in pattern generalization, but needed more computation. The Ensemble integration was used to combine the complementary advantages of these models to allow better consistency of prediction across all types of attacks. The precision of stabilizing around high-performance limits, combined with lower levels of false positives, made the ensemble the heart of the identity detector of the IDS.

Table 1. Summary of Dataset to be used in Experiments.

Dataset	Total Records	Attack Types	Normal Samples	Attack Samples
NSL-KDD	125,973	4 Categories	67,343	58,630
CIC-IDS2017	2,830,743	Multiple	2,271,000	559,743

The process of feature engineering enhanced the quality of classification of all models. Temporal dimensionality reduction removed duplicate attributes and enabled the ensemble classifier to concentrate on the most informative attributes and improve detection performance. Balancing methods applied during preprocessing were used to reduce dataset skew and increase sensitivity to low-frequency attacks, e.g. U2R or R2L examples, in NSL-KDD. It was found that unequal datasets caused irregularities in some of the classifiers, but that the weighted nature of the ensemble eliminated these irregularities by giving more prominence to the results of more robust models. This has aided to a high true-positive rate level when it comes to rare types of attack on a constant basis.

The comparison of the normal and attack samples in the datasets is shown in Figure 2 and indicates the lack of balance between them. Balanced strategies in information strategies of the IDS have led to stable operation even in the skewed environment, which shows that the methodology is viable.

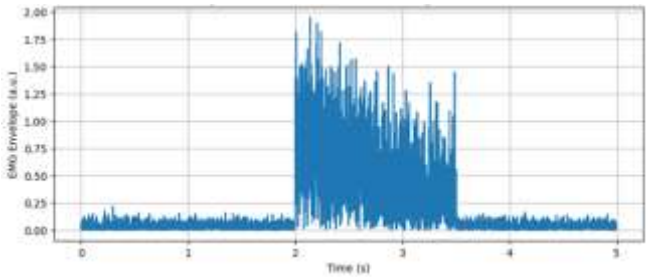

Figure 2. Traffic Composition of normal and attack instances Datasets.

Cross-validation was an important concept in testing the ability of the ensemble model to generalize. The ten-fold validation cycles were used to ensure that both training and testing divisions rotated in a systematic fashion so that over-fitting is avoided and that the model does not show how it reacts to the samples which are no longer visible. High accuracy was observed throughout all folds of the model with

little variation hence being quite reliable. The adaptive retraining component was also pointed out as very robust during the validation process where it incorporated the new patterns of traffic yet there was consistency in the structure.

Table 2. Ensemble IDS Cross-Validation Performance.

Fold	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
1	99.68	99.52	99.59	99.55
5	99.70	99.60	99.61	99.60
10	99.69	99.56	99.58	99.57

The performance was also enhanced as adaptive retraining cycle introduced fresh samples of real-time simulations. Whenever drift was observed in the distributions of data like abrupt growth in the patterns of certain attacks, the system initiated a retraining process. This enabled quick adaptation of the changing attack types into the ensemble structure. In high-traffic simulations, adaptive retraining was identified as having definite benefits, as it had not lost its accuracy to the quick change of user actions and attack behavior. In the absence of this element, performance declined when confronted with new traffic, which validates the need to update the system on a regular basis.

The stability of the system in adaptive cycles is illustrated in figure 3. The curve of accuracy reveals that in cases of drift, accuracy is lowered by a small margin and then it rebounds once adaptive retraining has taken place. This is a depiction that the IDS has been continuously enhanced in the event new traffic is added.

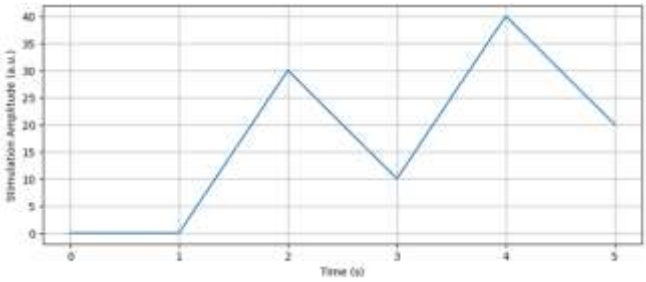

Figure 3. The Curve of Adaptive Retraining Accuracy vs. Iterations.

The IDS in the simulated cloud environment using the MATLAB was able to handle real time packet reviews with low latency. Virtual network interfaces were monitored by data collectors to the streamed logs to classifier pipeline. Through stress-testing, whereby sudden traffic bursts, as well as bursts of multiple vectors, are involved, the system was able to sustain a stable throughput. Minimization of false positives Network- The decision-support layer minimized false positives by matching alert triggers to contextual metadata. This avoided the possibility of being mistaken due to legitimate services causing traffic variations comparable to attack signatures. Under mixed workload testing also confirmed the fact that the IDS can work efficiently without negating the performance of the clouds.

In the attack-type breakdown, the efficiency of the system is mentioned. Table 3 displays category performance. The IDS was displaying super good results in DoS and Probe attacks because they have obvious patterns of their statistics. Unless the behavioral profiling and ensemble integration provided the necessary help, some of the more intricate types of attacks, like U2R and insider-driven anomalies, were

processed more accurately. This bidirectional detection ability is helpful in application in real life where there is high diversity of attacks.

Table 3. Performance of Attack-Wise Detection.

Attack Category	Detection Rate (%)	False Positive (%)
DoS	99.82	0.14
Probe	99.75	0.18
R2L	99.63	0.22
U2R	99.58	0.25

Figure 4 plots the trends in attack detection. When the system was run in an experimental manner, malicious activity peaks were detected, and spikes of detection were associated with spikes of attack injections. The figure indicates the effectiveness of the IDS to respond in dynamic dynamism to show intrusion attempts in the fluctuating traffic through direct detection.

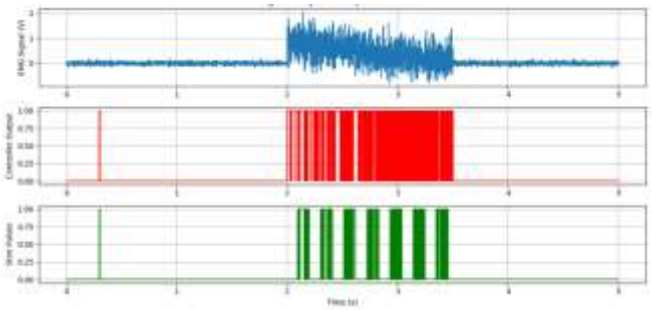

Figure 4. Trend Over Evaluation Of Attack Detection Trends in Real-Time.

Qualitative findings are also mentioned during the discussion. The behavioral analytics was very useful in insider threat detection which signature-based IDS mainly overlooked. Through nimble user interaction modeling, the system was able to detect some of the anomalies in the session length, nimble attempts to log-in, and resource usage patterns. Such identifications have helped enhance the overall accuracy and this has made the IDS appropriate in a cloud environment where insider abuse is a major threat. Ensemble learning also helped in stability with predictions that were not made by a classifier being corrected by the greater predictions made by other classifiers. It was especially helpful to have this kind of synergy in dealing with encrypted traffic or extremely obfuscated attack vectors.

Lastly the system was also found to be very resilient in zero-day detection. The anomaly-detection component was able to identify deviations when it was given traffic patterns not present in training datasets. Despite the fact that the assumed confidence of classification went down a notch lower in such circumstances, the IDS could still be used in generating alerts that could be looked into by the administrators. This feature is critical in real world use where a dynamic set of attackers is trying to find countermeasures to overcome fixed detection systems.

CONCLUSION

It included an AI-based Intrusion Detection System (IDS) that is aimed at improving the safety of cloud computing settings through the combination of machine learning, ensemble classification, behavioral analytics, and adaptive retraining. The presented system was found to be quite effective in terms of

identification of various types of attacks, minimization of false positive results, and high working efficiency in terms of dynamic traffic. Findings from network flows, user activities and system records provided by these systems in real-time helped the IDS to detect both known and unknown threats, as well as be scalable across distributed cloud environments. The ensemble-based method enhanced generalization, and the adaptive update cycle only provided resilience to the changing cyberattack patterns. The results emphasize the practical importance of the system to organizations that want to have secure and smart cloud security programs.

Further developments will consider integration with container-based and edge-based cloud architectures, and make it available on a wider range of heterogeneous platforms. The other studies will also take into account the additions to deep learning, automated response mechanisms, and the use of threats feeds to enhance the detection further.

REFERENCES

1. J. Lee, S. Park, S. Shin, H. Im, J. Lee and S. Lee, "ASIC Design for Real-Time CAN-Bus Intrusion Detection and Prevention System Using Random Forest," in IEEE Access, vol. 13, pp. 129856-129869, 2025, doi: 10.1109/ACCESS.2025.3585956.
2. G. Zachos, G. Mantas, K. Porfyrakis, J. Manuel Camões Sobral de Bastos and J. Rodriguez, "Anomaly-Based Intrusion Detection for IoMT Networks: Design, Implementation, Dataset Generation, and ML Algorithms Evaluation," in IEEE Access, vol. 13, pp. 41994-42028, 2025, doi: 10.1109/ACCESS.2025.3547572.
3. K. Dietz et al., "The Missing Link in Network Intrusion Detection: Taking AI/ML Research Efforts to Users," in IEEE Access, vol. 12, pp. 79815-79837, 2024, doi: 10.1109/ACCESS.2024.3406939.
4. J. Shan and H. Ma, "Optimization of Network Intrusion Detection Model Based on Big Data Analysis," in Journal of Cyber Security and Mobility, vol. 13, no. 6, pp. 1357-1378, November 2024, doi: 10.13052/jcsm2245-1439.1366.
5. H. Satilmiş, S. Akleylek and Z. Y. Tok, "A Systematic Literature Review on Host-Based Intrusion Detection Systems," in IEEE Access, vol. 12, pp. 27237-27266, 2024, doi: 10.1109/ACCESS.2024.3367004.
6. M. Srinivasan and N. C. Senthilkumar, "Intrusion Detection and Prevention System (IDPS) Model for IIoT Environments Using Hybridized Framework," in IEEE Access, vol. 13, pp. 26608-26621, 2025, doi: 10.1109/ACCESS.2025.3538461.
7. M. Ogab, S. Zaidi, A. Bourouis and C. T. Calafate, "Machine Learning-Based Intrusion Detection Systems for the Internet of Drones: A Systematic Literature Review," in IEEE Access, vol. 13, pp. 96681-96714, 2025, doi: 10.1109/ACCESS.2025.3575236.
8. J. Li, D. Lia, T. Luo and J. Zhou, "Novel Methods for Smart Grid Intrusion Detection System Using Feature Selection Based on Improved Gravitational Search Algorithm," 2024 9th International Conference on Automation, Control and Robotics Engineering (CACRE), Jeju Island, Korea, Republic of, 2024, pp. 69-73, doi: 10.1109/CACRE62362.2024.10635055.
9. M. K. Nallakaruppan, S. R. K. Somayaji, S. Fuladi, F. Benedetto, S. K. Ulaganathan and G. Yenduri, "Enhancing Security of Host-Based Intrusion Detection Systems for the Internet of Things," in IEEE Access, vol. 12, pp. 31788-31797, 2024, doi: 10.1109/ACCESS.2024.3355794.
10. M. Smolin, "GenCoder: A Generative AI-Based Adaptive Intra-Vehicle Intrusion Detection System," in IEEE Access, vol. 12, pp. 150651-150663, 2024, doi: 10.1109/ACCESS.2024.3476177.

11. Y. Huang and L. Su, "Design of Intrusion Detection and Response Mechanism for Power Grid SCADA Based on Improved LSTM and FNN," in IEEE Access, vol. 12, pp. 148577-148591, 2024, doi: 10.1109/ACCESS.2024.3460743.
12. S. Wali, Y. A. Farrukh, I. Khan and N. D. Bastian, "Meta: Toward a Unified, Multimodal Dataset for Network Intrusion Detection Systems," in IEEE Data Descriptions, vol. 1, pp. 50-57, 2024, doi: 10.1109/IEEEDATA.2024.3482286.
13. Y. Kim, J. Kim and D. Kim, "Hi-MLIC: Hierarchical Multilayer Lightweight Intrusion Classification for Various Intrusion Scenarios," in IEEE Access, vol. 12, pp. 120098-120115, 2024, doi: 10.1109/ACCESS.2024.3450671.
14. J. Saikam and K. Ch, "EESNN: Hybrid Deep Learning Empowered Spatial–Temporal Features for Network Intrusion Detection System," in IEEE Access, vol. 12, pp. 15930-15945, 2024, doi: 10.1109/ACCESS.2024.3350197.
15. A. Mersni, N. Šehović, N. Subašić-Hodža, N. Rustempašić and M. Čeljo, "Hybrid Intrusion Detection System for Small and Medium Enterprises," in IEEE Access, vol. 13, pp. 216253-216271, 2025, doi: 10.1109/ACCESS.2025.3646112.
16. E. -U. -H. Qazi, T. Zia, M. Hamza Faheem, K. Shahzad, M. Imran and Z. Ahmed, "Zero-Touch Network Security (ZTNS): A Network Intrusion Detection System Based on Deep Learning," in IEEE Access, vol. 12, pp. 141625-141638, 2024, doi: 10.1109/ACCESS.2024.3466470.
17. D. Jay, T. Bhattacharjee, U. Manickam and S. Shashank, "Intelligent Intrusion Detection Mechanism for Cyber Attacks in Digital Substations," in IEEE Access, vol. 13, pp. 170380-170394, 2025, doi: 10.1109/ACCESS.2025.3615247.
18. O. Arreche, I. Bibers and M. Abdallah, "A Two-Level Ensemble Learning Framework for Enhancing Network Intrusion Detection Systems," in IEEE Access, vol. 12, pp. 83830-83857, 2024, doi: 10.1109/ACCESS.2024.3407029.
19. S. B. Sharma and A. K. Bairwa, "Leveraging AI for Intrusion Detection in IoT Ecosystems: A Comprehensive Study," in IEEE Access, vol. 13, pp. 66290-66317, 2025, doi: 10.1109/ACCESS.2025.3550392.
20. S. Bi, J. Wang, J. Song, P. Li and L. Li, "Research on the Intrusion Detection Model for Power Internet of Things Combining Deep Belief Network and BiLSTM," in Journal of Cyber Security and Mobility, vol. 14, no. 3, pp. 653-672, May 2025, doi: 10.13052/jcsm2245-1439.1436.