International Journal of Applied Mathematics

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

BGMNET-SHSO TECHNIQUES: A NEXT-GENERATION HYBRID DEEP LEARNING AND SWARM OPTIMIZATION FRAMEWORK FOR CLOUD INTRUSION DETECTION WITH ENHANCED ACCURACY AND EFFICIENCY

Dr. K. Sundravadivelu,

Assistant Professor Department of Computer Science,

Madurai kamaraj University, Madurai, Tamil Nadu, India.

svadiveluk2021@gmail.com

https://orcid.org/0009-0001-9969-1571

Abstract

presently, cloud security has become the main concern because most sensitive data is being stored and processed by utilising the services of cloud computing. All existing algorithms in IDS technologies have recently undergone enhancements; however, they may still face significant challenges in detecting sophisticated, evolving cyber threats while handling high-dimensional data and optimising the computational resources of large-scale cloud systems. The major challenges in the design of existing IDS algorithms are that they are less adaptable for new types of attacks, their detection performance is far from optimal under varying network conditions, and they are inefficient in utilising computational resources, especially when operating in cloud environments with huge volumes of data. These limitations suggest a weakness in the ability of traditional systems to provide real-time, reliable security without overloading system resources or generating excessive false positives. In light of these challenges, this paper presents two new methods to improve cloud IDS performance and further reduce computational efficiency. First, the paper proposes Belief Gated Memory Net, BGMNet for intrusion detection, which fuses deep learning with gated memory mechanisms for more efficient detection of intricate attack patterns while ensuring crucial information does not get lost between time steps. First, the main contribution of BGMNet is non-static adaptation to continuous updates in network traffic with the aim of dichotomizing legitimate behavior from malicious behavior. Second, batch-size computation optimization in model training is proposed based on Shark Smell Optimization (ShSO). By drawing inspiration from the foraging mechanism of sharks, ShSO efficiently identifies the optimal batch size to improve the convergence rates of deep learning models, along with higher accuracy while reducing the computational costs.

Index Terms— Cloud Computing, Security, Intrusion Detection System (IDS), Deep Learning, Classification, and Optimization.

I. INTRODUCTION

Cloud computing is an innovative model in which several IT resources, including storage, networks, servers, and operating systems, are delivered to users via the internet. Further, this

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

model allows much flexibility in accessing and scaling computing resources, according to demand conditions, usually paid on a pay-as-you-use basis [1, 2]. Cloud computing represents three core service models, and they are: SaaS; IaaS, standing for applications and infrastructure management, respectively, and the varied levels of user needs. SaaS means providing access to applications directly to the end-user. IaaS just provides the basic computational resource supply for the users, such as VMs, data storage, networking, and so on. PaaS provides users with a development platform for composing applications; thus, the underlying infrastructure will be managed without interference from the user. These flexible service models have, therefore, opened the possibility of wide-based adoption and enabled faster deployment, scalability, and elasticity. Since demand fluctuates in an organization, users can upscale their resources in a very efficient way, which is considered quite beneficial in dynamic environments or organizations [3, 4]. Cloud computing rapid adoption doesn't come without challenges, especially about security. The wide utilization of cloud services brings critical vulnerabilities to most aspects of cloud systems, especially network functions that form the backbone for service delivery. Because of this, security measures should be very strong. The severest security threats involve data breaches, unauthorised access, and the loss of confidentiality or integrity [5]. Security-related problems worsen as most cyber-attacks recently have been enhanced in their sophistication and frequency while attempting to evade traditional security measures.

The rapidity of evolving cyber threats requires developing sophisticated IDS able to disclose and mitigate such kinds of attacks. IDS play a very important role in the detection of malicious activities or anomalies within a network, which may point to a security breach. In cloud environments, resources are shared and distributed, making network threats significantly difficult to notice and subdue [6]. Traditional security solutions-firewalls, encryption, and access controls-were devised in the past for small systems or those that could be isolated. The normal mechanisms fail in view of the unmanageable volume and complexity of today’s threats-especially in dynamic, cloud-based systems with workloads and traffic patterns that change rapidly. The simplicity and scalability of modern attacks have grown beyond traditional mechanisms [7, 8]. Attackers use much more sophisticated methods for entry beyond the set security controls, while growing interconnectivity across cloud systems automatically multiplies the potential attack surface. Intrusion detection and prevention have therefore become central to cloud security efforts. They need to identify everything from attempts at data exfiltration to denial-of-service attacks that might bypass traditional security solutions. Given the increased scaling up and diversification of cloud-based infrastructures, the need for deeper and more adaptive IDSs keeps waxing with each passing day.

More sophisticated, proactive solutions are therefore needed to meet these challenges. Machine learning, artificial intelligence, and advanced analytics make their way into the core of IDS to let it identify new patterns of malicious activity, adapt to emerging threats, and automate response actions. The modern methods of intrusion detection are focused on learning from large volumes of data generated within cloud environments that can further yield rich insights into attack behaviors, anomaly detection, and threat prediction [9]. This, therefore, reinforces the general security posture of cloud systems to be more attack-resistant. Consequently, IDS becomes pivotal in ensuring the security of cloud environments; nevertheless, its effectiveness

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

is pegged squarely on continued improvement of the algorithms used for detection and a deeper understanding of vulnerabilities and the threat landscape within the cloud environments. Cloud computing, due to the infrastructure complexity and heterogeneity of applications and services running on top of the cloud platforms, is inherently exposed to all types of modern cyber-attacks. Among these, the most serious and common risks include DoS, DDoS, and DNS attacks [10]. Normally, a reason for such an attack may be to disrupt normal cloud services, deny service to legitimate users, or degrade significant services. In a distributed DoS, malicious traffic is spread in a controlled manner over multiple sources; hence, it will be more difficult to trace and block. In turn, DNS attacks are those that manipulate the Domain Name System to make traffic move elsewhere surreptitiously: to force the users to land on malicious sites or to render a service unreachable [11, 12]. Since these services are increasingly integrated into key company processes, this could amount to a grave aftermath-a huge financial setback or even character and reputation damage.

This is because with an ever-increasing dependence on the cloud, starting from personal to enterprise applications, robust and efficient security has been cast centre stage as never before, while the number of devices and volume of data continue scaling. Traditional cybersecurity doesn't scale. Rule-based methods of checking security and, for that matter, even humans monitoring data are incapable of taming the scale and complexity of the modern cloud environment. The cloud ecosystem is dynamic, whereby applications keep interacting with users and devices on the move [13, 14]. This generates huge volumes of data that continuously need real-time analysis for detection and response against various threats. Hence, intrusion detection systems with automated means become an imperative ingredient in risk management and mitigation within cloud computing. In this case, IDS operates automation and, therefore, processes large volumes of information at much higher speeds and greater accuracy than human operators. Therefore, it quickens the process, whereby quicker identification of threats or any other form of attack is performed and quicker action against it. Regarding this, automated IDS becomes an imperative layer of defense that guarantees security with high availability in cloud services. However, no intrusion detection system can usefully be integrated into a cloud ecosystem before its robustness and functionality are thoroughly investigated. The cloud environment is peculiarly unique due to its high dynamics and multi-tenancy, which introduces scalability; thus, any IDS model developed for more static and isolated systems can never match the threats occurring in cloud infrastructure. It thus requires careful tailoring of IDS to needs and challenges presented by the cloud environment, including scaling traffic and data typical for cloud services, and at the same time being able to detect increasingly sophisticated and varied types of cyber-attacks that are prevalent in this space. IDS shall be designed to cater to multi-tenancy, which means multiple users shall share the same physical resources but keep operations isolated and secure [15]. The IDS needs to support discrimination of legitimate traffic from malicious activities without raising too many false positives or missing out on critical threats. Considering that cloud computing is complex and highly distributed, IDS must be equally agile, changing with the network topology and infrastructure so that protection scales and evolves continuously.

Robustness of IDS in cloud environments refers not only to their capability of threat detection but also to the competency of these systems to work without introducing considerable latency

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

or overhead. The IDS for cloud systems that support real-time applications or services based on high-performance requirements should run efficiently without interfering with any user experience or the performance of the whole system. Any effective IDS within the cloud would need to cooperate with other security technologies in providing multilayer defense while keeping pace with operational efficiency [16]. Considering that the cloud environments are ever-changing services, users, and applications are added day in and day the IDS should be flexible to adapt to these changes with as little manual intervention as possible. While doing so, the efficiency of the IDS in protecting cloud infrastructure and data rests on its detection capabilities; it also rests on how well it can integrate into the dynamic and ever-changing cloud ecosystem.

The rapid increase in cloud computing has brought new, serious security challenges, and an increase in the sophistication and scale of cyber-attacks on cloud infrastructures. This makes these attacks-DDoS, DNS spoofing, and data breaches among others-difficult to detect and mitigate amidst such unprecedented scale of cloud environments with increased usage of advanced evasion techniques by threats. Besides, all types of cloud-based applications and services generate huge amounts of data that ought to be analyzed in real time for detecting any potential security breach [17]. Since the cloud will continue to support a wide range of critical services and applications, the need for an efficient, scalable, and adaptive security framework is at a high level. Traditional IDS solutions fall behind this evolution, characterized by high false-positive rates, delay detection, and inefficiency to properly discriminate between real and malicious activity, especially in a real-time environment. This, as a result, would be to develop an IDS framework with a deep learning approach to make cloud computing strong, intelligent, and automated in understanding the sophistication and emerging nature of cyber threats. Because large volumes could be handled by deep learning models due to their intrinsic features, they hold great promise to enhance the performance of IDSs. Therefore, deep learning methods can promise much, and more precisely, neural networks do for anomaly detection, classification tasks, and pattern recognition, with important parts of network intrusion identification. That is motivated by the fact that these models have the potential to enhance accuracy and efficiency of the IDS by reducing false positives, high-speed detection, and proactive threat detection capabilities. All this makes the deep learning-based framework suitable for cloud environments that are ever-evolving and boundless. The IDS framework proposed herein uses deep learning for a more holistic, reliable, and scalable security solution against ever-evolving cybersecurity challenges arising in cloud computing.

This paper is organized as follows: Section 2 gives a short review of various proposed machine learning and deep learning-based IDS models, pointing out their strong points and limitations together with evolving trends in this domain. Section 3 elaborates on the proposed deep learning-based IDS framework and its architecture, underlying methodologies, and ways through which it addresses the limitations of conventional IDS models in cloud environments. The results obtained and their comparison with the analysis is presented in Section 4. It mainly probes into how well the proposed framework performs-in contrast to the traditional IDS models-along multiple metrics of detection accuracy, false positives, and computational efficiency. The last section, Section 5, summarizes some of the key findings and contributions made in this paper, while stating the direction for future work to be done toward further

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

improvements to be made in the proposed IDS framework and its applicability against evolving cybersecurity challenges.

II. Related Works

In recent years, the field of IDS has undergone a sea of change, as almost all traditional methods-like signature-based and rule-based ones-start to be represented by few older systems that were replaced by the ML/DL methods. Earlier IDS models relied fundamentally on some predefined attack signatures or rules to identify the threats. These methods have performed quite well in case of known attacks but proved less effective to find out new or unseen threats. However, these models still exhibited limitations in feature engineering, scalability, and handling complex attack patterns. Of late, IDS has been increasingly addressed by applying deep learning techniques. Deep learning is a class of machine learning which makes use of the power of neural networks: multiple layers used to represent high-level features directly from raw data in such a way that the necessity for manual feature engineering becomes null. These deep learning-based IDSs can learn complex patterns from big and high-dimensional data; hence, they find suitable applications in cloud environments where data volumes and complexity are much higher than in traditional systems. Recent studies have shown that deep learning-based approaches can effectively enhance detection accuracy and reduce false positives-arguably two of the most common challenges with traditional IDS methods. However, deep learning can hardly be deployed into IDS, since most of the deep learning techniques require large-sized labeled datasets for training and are afflicted with problems such as computational complexity and model decision interpretability.

The proof given by the authors [18] of the research is quite convincing and allows looking at DNNs as very prospective to enhance cloud infrastructures' security, especially against the ever-growing threat of DDoS attacks. This work has underlined the importance of DNNs in improving detection accuracy for robust security in a cloud environment. These DDoS attacks are turning out to be a serious challenge in cloud security day by day due to the increase in their frequency and sophistication, and traditional intrusion detection methods usually cannot keep pace with these evolving threats. The authors propose a DNN-based model that improves the accuracy of the detection mechanism and significantly enhances its efficiency for better applicability in large-scale cloud environments. The other point worthy of mention is that the authors have chosen the NSL-KDD dataset to test the model. This dataset is a recognized standard in intrusion detection research; for this reason, the coverage is complete for a wide range of attack types, including DDoS. Therefore, using the dataset is helpful in allowing the authors to test whether the model is suitable for detecting real-world attack scenarios. The main strengths of the proposed DNN model are in their autonomous learning of complex network traffic data, whereby the model provides efficiency in detecting known and unknown attack vectors.

Ali, et al [19] propose a state-of-the-art intrusion detection approach in cloud computing environments through a deep learning architecture, using CNNs, committed to finding the solution to specific challenges in cloud computing security. Traditional IDSs retain only rule-based or signature-based detection mechanisms that cannot detect new and sophisticated types of threats. This is in contrast to the CNN-based IDS of the authors, which relies on the

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

automatic learning of hierarchical features from raw data using the network; hence, their approach of threat detection is more flexible and dynamic. The major contribution of this research is that it trains the CNN with a representative and diverse set of datasets, both normal network traffic and various types of attacks collected from cloud environments. In that way, the authors make the model explore as many possibilities as may be proposed, so it could easily notice any deviation from normal behavior that might indicate a potential intrusion. That is very important with respect to cloud computing, where the dynamic nature of the network-being distributed-complicates the security landscape. The proposed CNN-based system is much more adaptable to the ever-changing characteristics of cloud-based attacks. In contrast with the traditional IDS models, which rely on predefined rules or signatures, the CNN model itself extracts useful features from the raw data it will be fed with; thus, it is allowed to be even more successful in detecting both known and unknown threats. Being able to self-learn and generalize from the data automatically makes this a considerable advantage in respect to identification of previously unseen attack patterns. It also points out that the study indicates the possibility of CNN reducing false positives of traditional IDS methods through improved attack detection.

Biswas, et al [20] propose a new paradigm in intrusion detection in cloud computing through the development of machine learning techniques, with special emphasis on hybrid methods of feature selection. As cloud computing is one of the fast-emerging architectures that distribute resources over the internet, the system becomes prone to a lot of security vulnerabilities; DDoS and DoS attacks are also prominent among them. One of the most useful points of this research was the integration of hybrid feature selection techniques with the aim of enhancing efficiency and accuracy in IDS. In this line, the authors express the use of different hybrid techniques of independent dimension reduction, which might give better learning while focusing on the most informative features for attack detection. Real-time intrusion detection in cloud environments remains a challenge due to large volumes and varieties of data. The proposed IDS framework is implemented with these hybrid feature selection methods to increase the detection accuracy and ensure the feasibility of the system in real time, addressing the dynamic nature of cloud computing environments. Devi, et al [21] provided a detailed discussion of the various strategies adopted by different IDS and put forth a discussion on the growing security risks associated with network infrastructures which are continuously increasing their circumference. The modern computer networks are growing at an unbelievable rate and, therefore, the need for efficient and robust intrusion detection is becoming more crucial than ever. However, several IDSs have been proposed, which aim at growing security and privacy challenges that cloud computing and other networked environments are suffering from. The authors insist that much as the development of robust defense systems is important, a lot of work needs to be done in enhancing the datasets used for the training and testing of these security solutions. They say, in turn, that enhanced datasets are necessary for refining the offline and online IDS models, which would be more competent in detecting complex and continuously evolving threats. One of the most important contributions of this work is giving special importance to publicly available network-based IDS datasets. It is emphasized that the quality and diversity of the dataset applied are crucial for IDS detection accuracy. This research gives a clear insight into various strengths and weaknesses associated with the datasets by conducting an in-depth study

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

of these datasets, hence proving to be very useful for research work in the development of IDS. Also, this study identified the need to integrate state-of-the-art deep learning techniques into the IDS to improve the security of the IDS systems.

Alijuaid, et al [22] point out the importance of Intrusion Detection Systems in defense mechanisms against cyberattacks within cloud computing environments. While the scale of network traffic keeps growing, existing IDS solutions still face various challenges regarding efficient processing and analysis of huge volumes of data common for cloud infrastructures. It is this very complexity that results in less effective detection accuracy of attacks, more so with dynamism in the varying cloud environment settings. Finding such multidimensional challenges a reason good enough, the authors introduce a new deep learning-based model comprising an advanced CNN architecture, which has been provisioned for the efficient detection of cyberattacks within the cloud. Proposed CNN-based architecture will inherit the strengths of the CNN architecture to learn features from large volumes of big data in a meaningful way. The authors have proposed the model with some key stages, which include dataset collection followed by preprocessing as an important step towards making the data quality and relevance appropriate for use in the training of the deep learning model. CNN architecture is especially suited to finding the spatial hierarchies and patterns that underlying data portray. In intrusion detection for cloud environments, this subtlety in the extracted features positions CNNs better to perform the task of detecting even subtle and complex attack signatures that could have been overlooked through traditional rule-based or signature-based methods. Zhang, et al [23] gives a detailed methodology on every component of the framework: how the fuzzy logic system selects features, the optimization process of SSA, the architecture of DBN, and how GRU is integrated with CNNs. All these elements are strongly connected in enhancing this model's capability for the efficient detection and classification of various attacks in network traffic. This empowers the system even more by chronological SSA-optimized DBN, enabling the network to learn powerfully from sequential data. The SSA optimization ensures the fine-tuning of the DBN parameters so that better performance can be achieved concerning intrusion detection. Again, the incorporation of GRU with CNNs implores dynamic capturing of the temporal dependencies in network traffic, enhancing the model's capability to detect attacks with varying temporal patterns.

Hasimi, et al [24] have proposed a feed-forward propagation Artificial Neural Network model for improvement in cloud security. The main steps that are very essential for integrating these models within the existing cloud security strategies are studied. Deep learning techniques like ANN have given cloud security a major facelift as far as detection and prevention of cyber-attacks are concerned. However, the authors emphasize that successful applications of such techniques depend on one crucial variable: computational resource requirements, costs of collection and preparation of data, development complexity of models, continuous integration, and maintenance efforts. The authors underline that efficiency in the ANN model for cloud security is ensured dependent on a number of aspects such as, but not limited to, quality in training data, architecture design, and weight adjustment algorithms. The quality of the training data forms a prominent factor, most importantly, in determining the learning of the model for the best representation of both legitimate and malicious network traffic. This study uses the

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

dataset taken from the most recognized source in relation to machine learning datasets: Kaggle, which will help contrast the performance of the ANN model.

Chaudhari, et al [25] propose a new intrusion detection framework for meeting the challenges of attack detection, which keeps on evolving in VM environments where malicious running processes may try to hide from the traditional security mechanisms. Classic IDSs have been developed for attacking detection, based on predefined behavior patterns. However, most of them are facing difficulties in detecting unknown or novel attacks, especially in the case of VMs. In this regard, the authors have identified improving IDSs with state-of-the-art ML/DL techniques to counter this growing menace. The suggested architecture is focused on system calls sequence analysis for detecting both known and unknown attacks. System calls are one of the vital activity indicators of different applications and processes; therefore, its analysis has been considered one of the promising directions for malicious activities detection. In this paper, the authors intend to take leverage of a hybrid model, one which uses LSTM networks and anomaly detection combined with system call frequency for the capture of temporal dependencies in system calls, so important in locating suspicious patterns over time.

The current literature on IDS has, to a large extent, enhanced security in many computing environments. However, gaps exist regarding the important issues that have an implication of breaking this security mode, particularly in cloud computing and virtualized environments. Most traditional IDSs depend on predefined patterns of behavior and signature-based techniques facing inefficiency in finding their way toward detection in novel, sophisticated, or zero-day attacks. These methods suffer from problems related to scalability, adaptability, and dynamic issues that are inherent in modern cloud systems, where new types of attacks are emerging continuously. Besides, their performance normally degrades under high-volume traffic conditions typical for a cloud environment that demands processing huge volumes of data in real time. These challenges seem to have a promising solution with the use of ML and DL techniques for enabling intrusion detection systems that are much more adaptive and scalable. Most of the current solutions target either small-scale or isolated environments, with very limited consideration for complexity in cloud infrastructures. Secondly, most ML and DL models are still dependent on conventional datasets, which in most cases are static and may not represent the diversity and dynamism of real-world cloud network traffic. These models also tend to miss out on the subtleties of system call behavior in virtualized environments, wherein attacks can mask themselves within the cloak of legitimacy of system processes and hence are difficult for traditional IDSs to spot. Another literature gap is related to the hybrid technique integration, which combines strengths from different ML and DL methods. Though hybrid models-like LSTM networks combined with anomaly detection-have shown a growing interest, they still remain in the embryo stage of development. Above all, most of these hybrid systems have not leveraged the full potential in capturing temporal dependencies and statistical anomalies in real-time data with a view to optimize it for cloud environments, especially in order to detect unknown or sophisticated attacks.

III. Proposed Methodology

This section introduces two newly proposed approaches for intrusion detection in cloud systems. First is the Belief Gated Memory Network, BGMNet; it will be using the powers of

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

deep learning and memory networks to correctly identify intrusions within cloud environments. In line with the classic IDS approach, BGMNet extends this model with a belief-based mechanism that may refresh, at runtime, the understanding of the model in network traffic patterns. Of these, the second one is Shark Smell Optimization, ShSO-a new type of optimization technique applied in the problem of batch size computation in IDS. ShSO takes its inspiration from sharks because of their distinctive predation instinct, and it emulates their sensing capability in tracking down the optimal solutions in complex search spaces. It does so by embedding a bioinspired optimization into the batch size selection process, while improving model training performance with reduced computational cost. This synergy provided by BGMNet and ShSO gives a significant boost within the landscape of the existing methods of IDS by offering higher accuracy, faster training, and better efficiency in cloud-based environments. The overall working of the proposed cloud security system is given in Fig 1.

A. Belief Gated Memory Net (BGMNet)

Belief-Gated Memory Net (BGMNet) is a novel hybrid deep learning model for sophisticated and dynamic intrusion detection in cloud systems. The model synergically combines hierarchical feature extraction capabilities of DBNs with the power of capturing temporal dependencies using gated memory mechanisms such as LSTMs or GRUs. The main innovation of BGMNet can be summarized as the successful integration of the strength of DBNs unsupervised feature learning with the strength of the gated recurrent units for sequential processing, providing a system capable of analyzing network traffic in space and time with quite good precision. Given the DBNs for hierarchical representation learning, the model can automatically learn from the complex and sophisticated features in network-raw data such as system logs and packet flows without handmade feature engineering. Meanwhile, memory units gated by time enable the model to take time-dependent behaviors into consideration, thus guaranteeing that even small temporal patterns that indicate intrusions are caught effectively for analysis. Another novelty of BGMNet is its dual-layer mechanism for intrusion detection. Whereas most current methods of intrusion detection involve only one pass either for anomaly detection or for static pattern recognition, BGMNet detects potential intrusions on two complementary levels: First, the DBN component captures global patterns across various dimensions of the input data, building a strong feature set that encompasses both benign and malicious behaviors in the cloud environment. While doing that, the gated memory units focus on the time-series data of sequentially related dependencies that may indicate gradual or delayed attack vectors, such as low-and-slow DDoS attacks or APTs. In this respect, the model is guaranteed to find not only immediate anomalies but also predict and ward off emerging threats-most effective in the evolving landscape of cloud computing security.

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

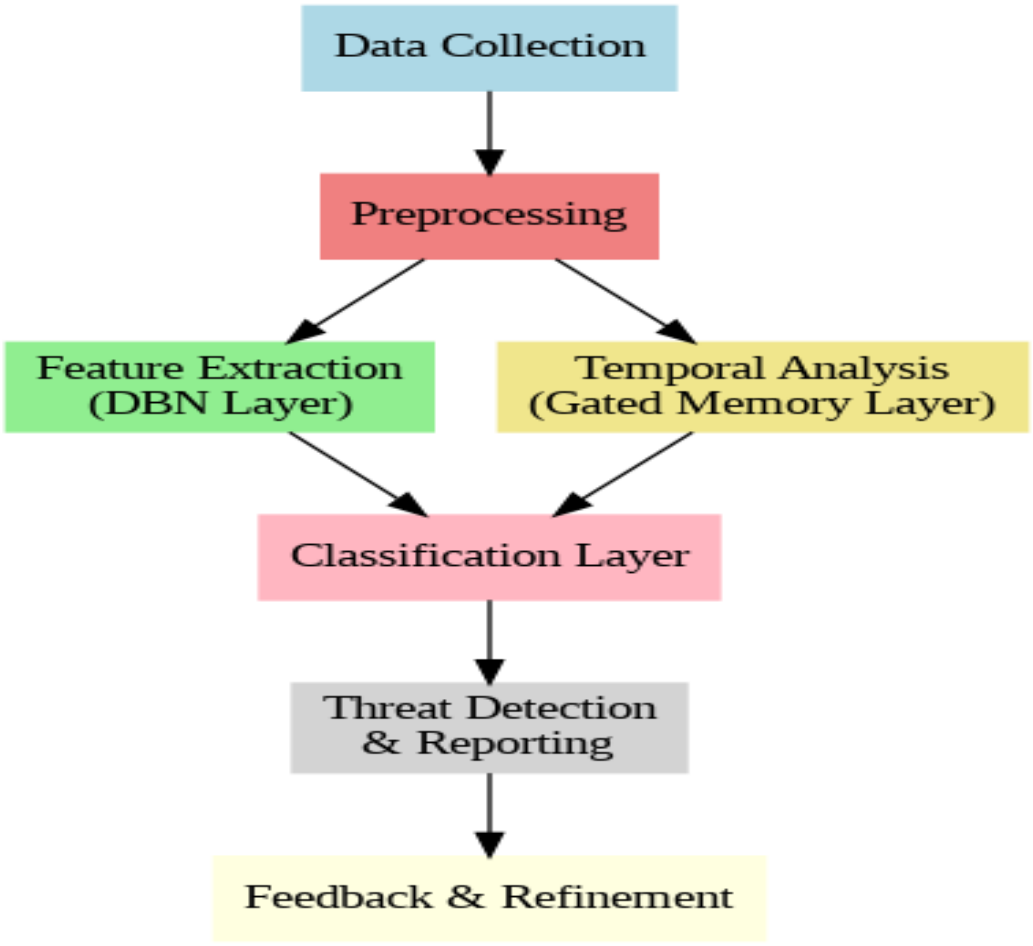

Fig 1. Overview of the proposed cloud security system

BGMNet has critical advantages in intrusion detection among the cloud systems. High-dimensional voluminous data characteristics of cloud environments are dynamic in nature and come from various sources like virtual machines, containers, and network devices. It is observed that traditional intrusion detection systems cannot bear such complexity, especially when unknown attack patterns pop up or are encrypted. BGMNet does exceptionally well in these cases due to its hybrid architecture. While the DBN layers are able to find the hidden relationships from high-dimensional datasets, the gated memory units specialize in anomaly detection across time, independent of data type or encryption. The twin capability so positions BGMNet among state-of-the-art solutions toward the protection of cloud systems from both known and zero-day threats. Unique properties in BGMNet are intrinsic adaptiveness and efficiency. Previous works, except pure CNNs or LSTMs, cannot combine the analysis of spatial and temporal smoothly. While CNNs are very powerful in the analysis of static data, they fail to capture sequential dependencies; on the other hand, LSTMs, performing very well in temporal analysis, may completely miss essential spatial patterns which could be highly relevant for intrusion detection. BGMNet achieves this by being at the intersection of both paradigms, providing a unified model with broader data analysis capability.

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

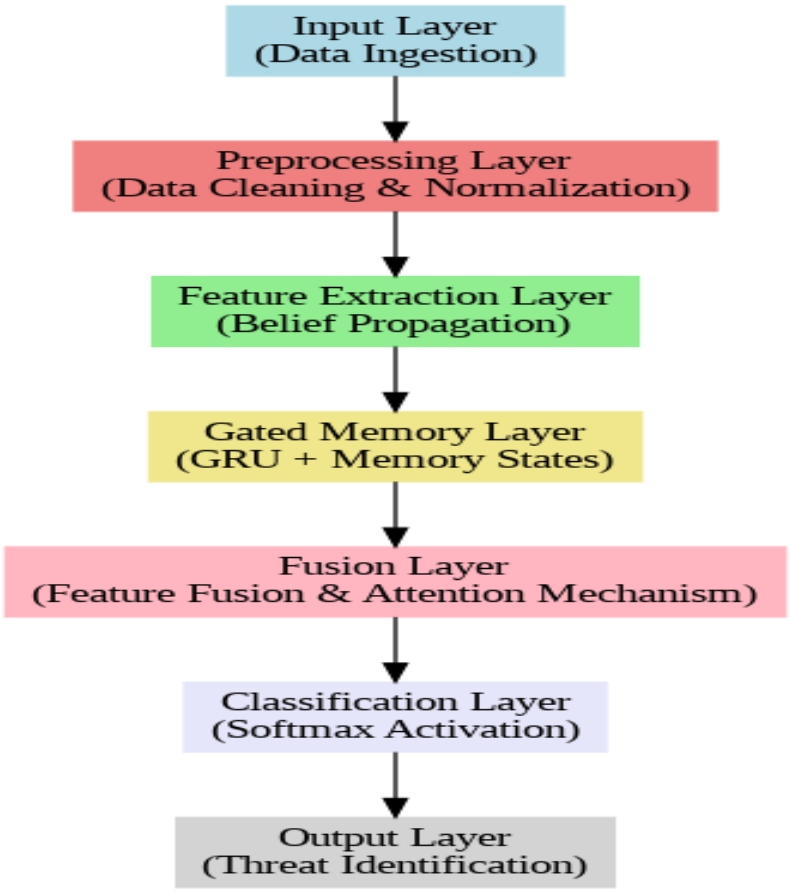

Fig 2. Flow of BGMNet

Further, having DBNs as part of the architecture ensures that feature learning has only an unsupervised reliance, reducing dependence on labeled data, hence generalizing to many different datasets more easily. It is even critical in cloud systems, as most of the time, large diversity and heterogeneity among data sources have often caused many problems to classical models. To wrap it up, BGMNet presents a paradigm shift to intrusion detection in cloud systems because its architecture integrates deep belief networks and gated memory units in a way as to handle both spatial and temporal dimensions of cyber threats these days. The adaptability of the model for various data types, further combined with its ability to learn both static and dynamic features automatically, offers a guarantee of superior performance against existing methods. As computing in the cloud is still proliferating, BGMNet has provided an efficient and reliable framework for safeguarding these infrastructures against attacks of burgeoning sophistication. It is particularly suitable for cloud security, insofar as it can handle special challenges wrought by the cloud environment. In the context of unsupervised feature extraction and sequential anomaly detection, the proposed BGMNet will combine the strength of DBNs with that of memory mechanisms with gates. This duality capability is enabled by the fact that BGMNet can detect both known and novel threats while ensuring computational efficiency relevant to large-scale cloud systems.

As shown in Fig 2, data pre-processing is the first step in the flow of BGMNet. It collects raw cloud traffic logs-data, network packets, system calls, user activities-from various nodes within the cloud ecosystem. As the nature of cloud data is heterogeneous, so different preprocessing

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

steps are required for cleaning, normalization, and encoding in a uniform input format so that it would be compatible for different kinds of inputs such as numerical metrics and textual logs. The data pre-processed thereby is fed to the unsupervised feature learning of the Deep Belief Network layer. In this regard, DBN consists of a stack of several Restricted Boltzmann Machine layers, each of which is trained to extract hierarchical features representative of the inherent pattern of both normal and malicious behaviors. For instance, DBNs are capable of finding statistical anomalies in network traffic, which in general would point to an imminent attack, such as sudden and unexpected packet size spikes or unusual port activities-common attributes of DDoS or brute-force-type attacks.

B. Shark Smell Optimization (ShSO) for Batch Size Computation

The proposed Shark Smell Optimization (ShSO) approach can be said to be a new methodology for the estimation of batch size, which will be able to find out the runtime optimal batch size for BGMNet, which is a hybrid deep learning model of state-of-the-art nature for enhancement in intrusion detection in cloud systems. ShSO looks to leverage that efficiency and precision in a bio-inspired shark sensory mechanism whereby sharks detect and respond to stimuli with utmost accuracy and speed. This actuates like the natural capability of the shark to adjust its hunting strategy, given environmental cues; this adaptiveness of the shark is put into place in how incoming data batches are dealt with in training within this model. BGMNet follows a hybrid architecture that embraces a number of building blocks like RNN and memory networks for developing a robust dynamic intrusion detection system in cloud environments. Intrusion Detection in cloud systems faces the dual challenge of volume-speed-accuracy with low computational overhead. Batch size is one of the most important hyper-parameters which control the number of training examples processed prior to updating the model weights, and its work flow is given in Fig 3.

The result could be a reduced batch size that gives higher frequency updates, thus making the process of training even more agile but, possibly noisier. That is, ShSO "sniffs" the environment by tracking KPIs of interest, including loss reduction, gradient stability, and computational efficiency, and changes batch size in response to these metrics. The ShSO technique can adapt itself to the changing cloud environments where the nature of the incoming data may fluctuate and system conditions concerning available memory and processing power change. With dynamic computation of the optimal batch size, ShSO guarantees that BGMNet performs well consistently under different conditions. This technique is well-suited to the overall architecture of the BGMNet, as it increases the capability for the detection and response against sophisticated intrusion patterns in the cloud system. Basically, Shark Smell Optimization for Batch Size Computation enhances the training efficiency of the BGMNet model and aligns with real-time adaptive, behavior-mimicking nature to make its responses dynamic-and all the more suitable for the ever-evolving and complex landscape of cloud-based intrusion detection. ShSO for batch size computation has significant advantages compared to the traditional methods of optimization for deep learning, especially in a dynamic and complex task like intrusion detection in cloud systems.

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

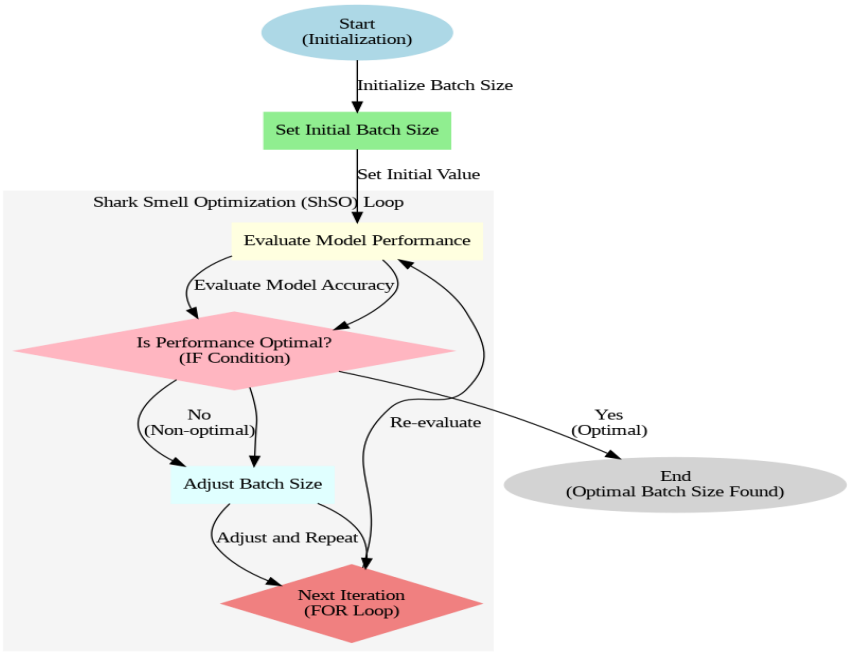

Fig 3. Flow of ShSO technique

Classic optimization methods for batch size determination, such as fixed-size or learning-rate schedules, fail to adapt to the changing dynamics within the training process. While ShSO introduces flexibility and intelligence to the technique, taking a leaf from nature, with allowance for real-time dynamic adjustments of the batch size during training, its adaptive nature guarantees handling different complexities of data, network conditions, and computational constraints with much better efficiency. Most importantly, ShSO has the key advantage that it can automatically optimize batch size with very minimal human intervention and tuning. Using the grid search or manual selection of batch sizes is computationally expensive; it also requires a lot of expertise to find an optimal configuration using existing methods. On the contrary, ShSO applies its inspiration from nature in modeling the shark's natural capability for detection and tracking of certain environmental cues to enable the model to work independently by automatically changing the batch size in accordance with the current state of the model and data. This will be important in cloud environments where the volume of data may be very large and highly variable and the available computing resources vary depending on system load. Traditional methods can hardly manage such a balance, while it will result in either inefficient processing or convergence much more slowly; ShSO optimizes this in real time.

IV. Results and Discussion

Herein, we show the performance of our proposed model on the three benchmark datasets: NSL-KDD, CICIDS2017, and CICIoT2023. The NSL-KDD dataset was an improved version of the KDD Cup 1999 dataset to have a better distribution that avoids class imbalance problems and unnecessary records. The CICIDS2017 dataset was generated by the Canadian Institute for Cybersecurity, including complete captured network traffic with most up-to-date attack scenarios such as DDoS, DoS, port scans, and botnet activities. A similar dataset, provided by the Canadian Institute for Cybersecurity, is the CICIoT2023, related to the security of Internet

Received: August 07 2025

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

of Things networks. In this dataset, traffic data from IoT devices in smart home environments is considered. Several attack scenarios are provided as spoofing, flooding, and reconnaissance attacks. It will have much value in evaluating intrusion detection model performance in IoT contexts, as heterogeneity and resource constraints pose additional challenges.

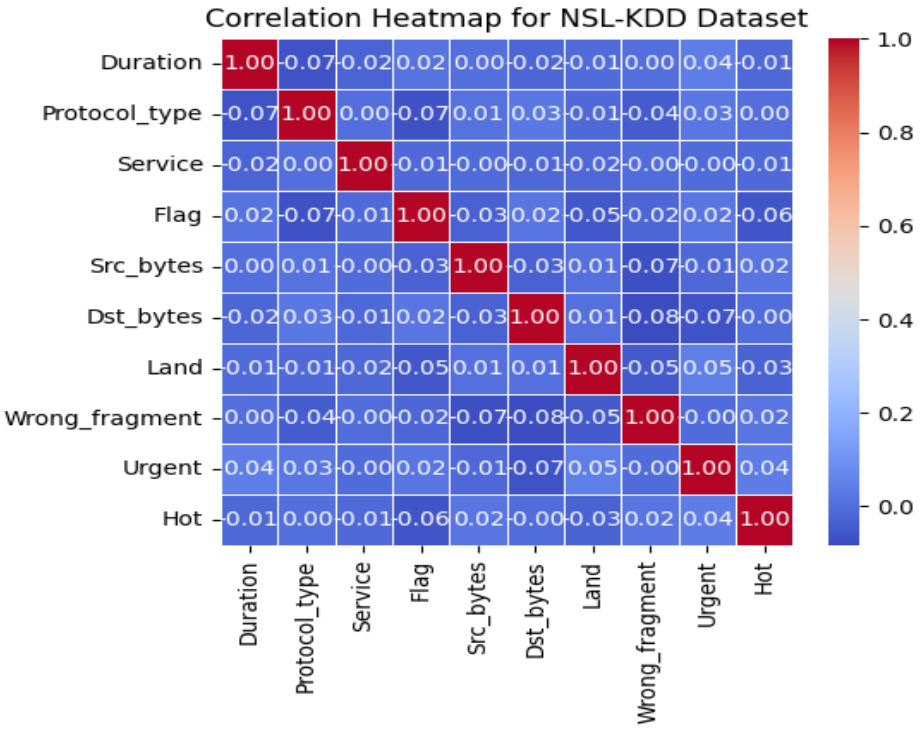

Fig 4. Correlation analysis for NSL-KDD dataset

Fig 4 provides an overview of how the selected features interact with each other, offering insight into the dependency of every feature of network traffic on others. Among the given dataset, key features such as Duration, Protocol type, Service, Src_bytes, and Dst_bytes have different scales of correlation. For example, Src_bytes and Dst_bytes are bound to have a high correlation since both are about the amount of data transmitted between source and destination. The feature that is expected to be less correlated with other features includes Land, Wrong fragment, and Urgent because their settings reflect specific anomaly-related behaviours rather than general patterns in the traffic. This analysis of correlation helps feature selection to reduce the dimensionality in order to enhance the performance of the network intrusion detection models. Fig 5 depicts the correlation analysis based on the CICIDS-2017 dataset, which was developed to capture a wide range of network traffic behaviors to develop the detection of traditional and modern network attacks. Some of its features are Flow_duration, Total_fwd_packets, Total_bwd_packets, and Flow_bytes_per_second. High positive correlation of Flow_duration with Total_fwd_bytes indicates that longer flows tend to carry more data, which could be expected in the case of legitimate extended network sessions. Highly correlated Flow_packets_per_second and Flow_bytes_per_second features indicate that higher data rates normally correspond to higher packet transmission rates.

Received: August 07 2025

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

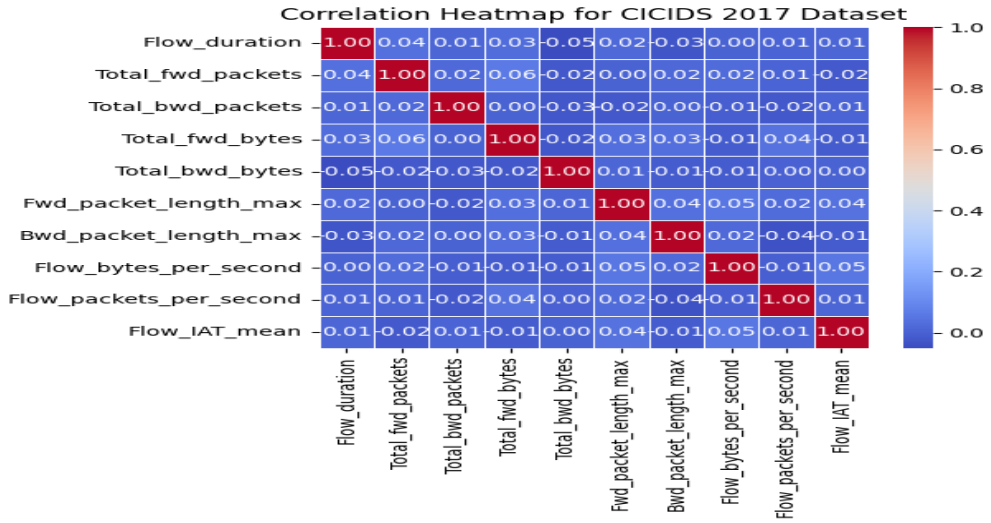

Fig. 5. Correlation analysis for CICIDS-2017 dataset

Fig 6 illustrates the correlations between Flow duration, Packets sent, Sent bytes, Source IP, and Protocol features. The Flow_duration and Sent bytes present a medium correlation value, which is comprehensible because longer flows mean more data are sent. Similarly, in this respect, Flow_bytes_per_second and Flow_packets_per_second present standard behavior for IoT devices: the higher the volume, the bigger the packet rate. The features Source IP and Destination IP have a very important role in identifying anomalous connections. Probably, this correlation helps in identifying unauthorized devices or compromised IoT nodes. By knowing how each feature influences the other, a security practitioner will be able to design effective models for the detection of such attacks like DDoS, botnet activity, or unauthorized access in IoT environments. In order to find the most prevailing features for threat detection in an ever-increasingly complex IoT network, such a correlation analysis is required.

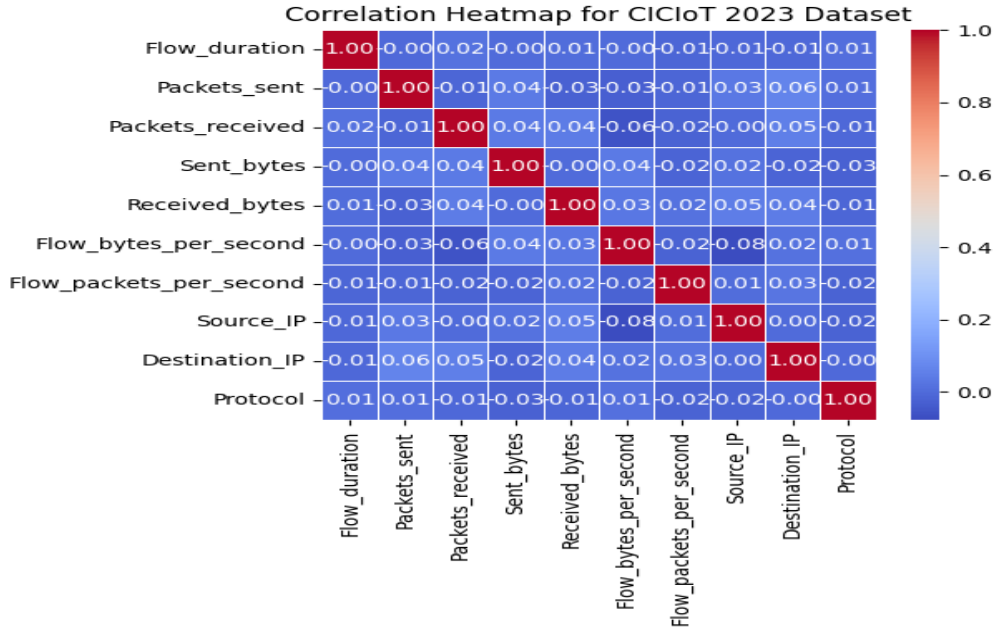

Fig 6. Correlation analysis for CICIoT dataset

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

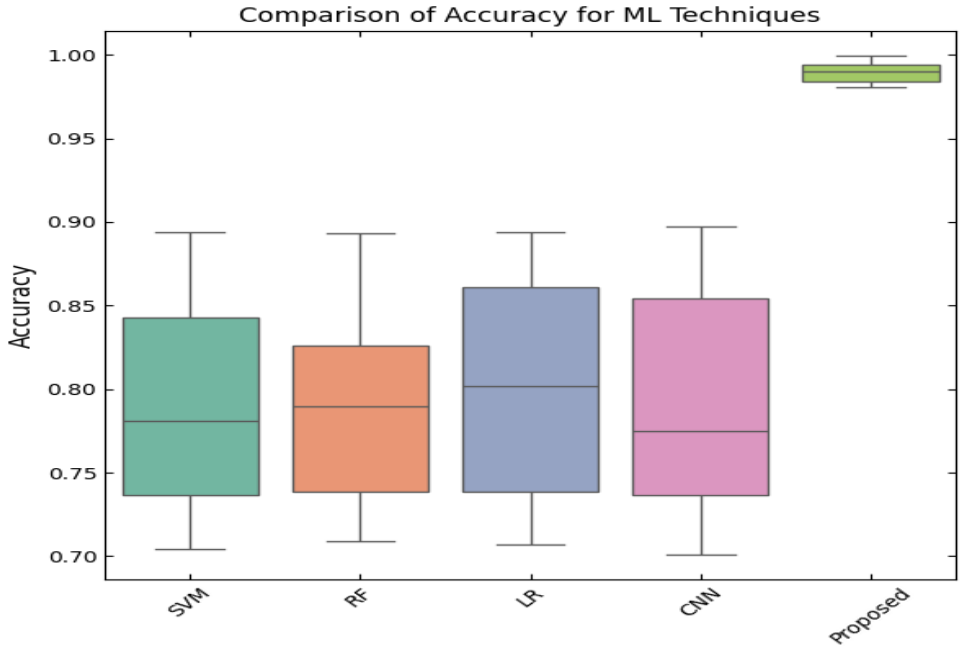

Fig 7. Accuracy comparison with machine learning models

Fig 7 compares the accuracies obtained from different machine learning models, namely SVM, RF, LR, CNN, and Proposed. Whereas accuracies of the previous models like SVM, RF, LR, CNN, etc., lie in the range between 70% and 90%, the accuracies of the proposed model are above 98%. Fig 8 compares various models in terms of their precisions. For example, the proposed model has kept portraying its excellent performance by precision values all above 98%. Whereas, results for traditional models such as SVM, RF, LR, and CNN are comparatively low, ranging from 70% to 90%. High precision of the proposed model denotes that this model is strongly capable of minimizing false positives.

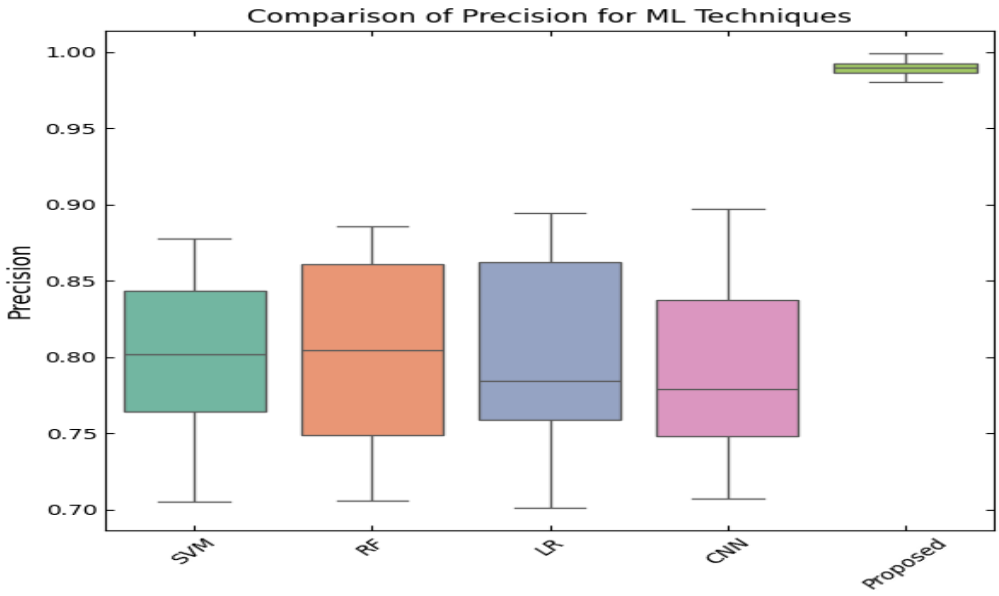

Fig 8. Precision comparison with machine learning models

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

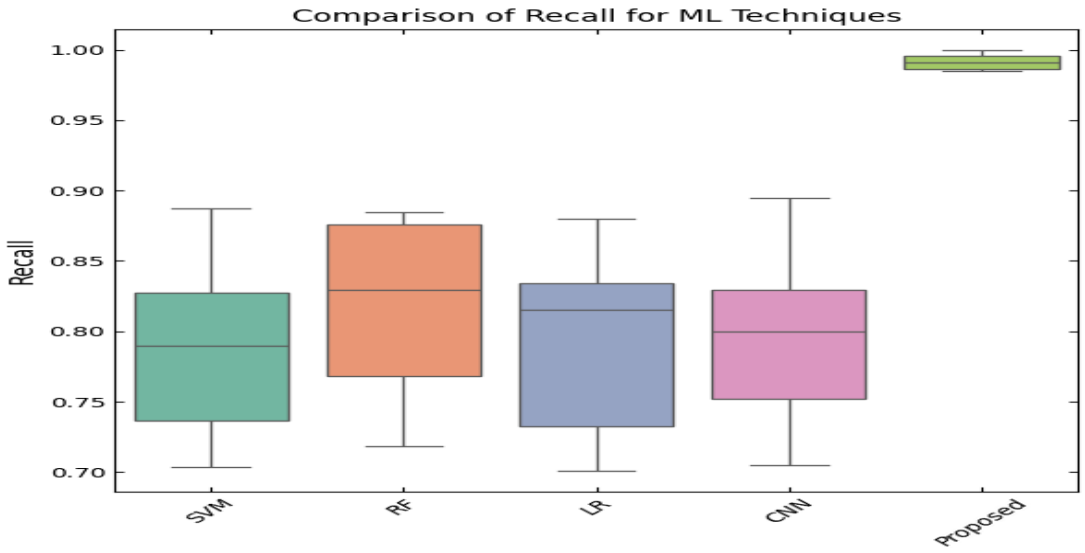

Fig 9. Recall comparison with machine learning models

Thus, it will be highly suitable for applications where the cost of false positives is costly, for example, intrusion detection or fraud detection systems. Fig 9 shows the recall comparison among models. That means the proposed model is doing very well, shown by highlighting nearly all the true positives to reduce false negativity risks. On the other hand, state-of-the-art models like SVM, RF, LR, and CNN have good but lower recall values compared to the proposed model. The generally obtained range in these models is between 70% and 90%. This illustrates the fact that even though these models detect a good share of positive instances, they fail to detect some of them-which might be crucial in applications related to malware detection or the prevention of cyber-attacks. With the Proposed model's high recall, it will have a more inclusive capability for detection; hence, making it a better option for critical tasks where the missing of positive instances may lead to huge, disastrous consequences. As shown in Fig 10, performance comparison of different machine learning models, RNNBiLSTM, BiLSTM, LSTMFCNN, CNN+LSTM, CNN+BiLSTM, CNN_Contrastive, SICNN [26] , and Proposed technique on the CICIDS 2017 dataset using accuracy, precision, recall, and F1-score.

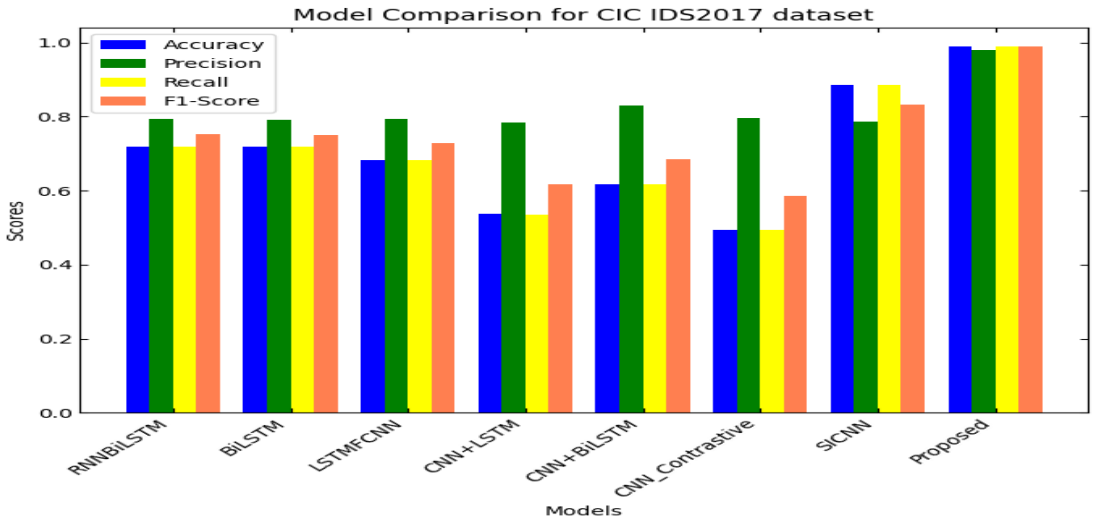

Fig 10. Model comparison using CICIDS 2017 dataset

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

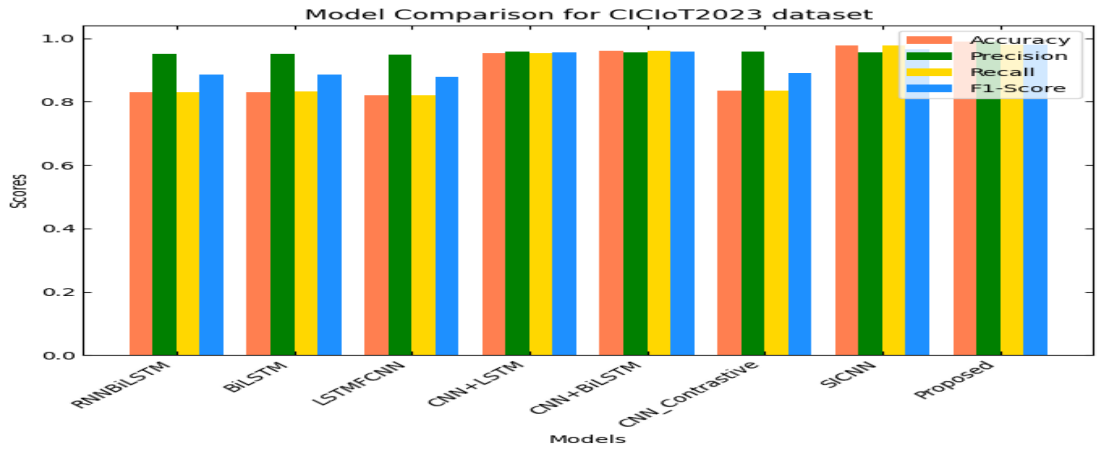

Fig 11. Model comparison using CICIoT-2023 dataset

Among all the models, the proposed model is distinguished with the maximum value in all metrics, having a great percentage accuracy of 98.9%, precision of 98%, recall of 99%, and F1-score of 98.9%. This means that the proposed model is capable of capturing and classifying data with the least error effectively. Models like CNN+LSTM and CNN Contrastive do well in terms of their accuracy but once again fail to beat the Proposed model on recall and F1-score too, showcasing that these models, though doing decently regarding the overall classification performance, still fail in detecting a pretty reasonable number of instances. Since the performance of the proposed model is far better, it is obvious that this model is extracting the features in a much more robust and deep manner compared to others. Thus, for complex classifications, the proposed model will be more reliable compared to other models. In Fig 11, the results from CICIDS 2017 prove that the proposed model also outperforms the other models on all the evaluation metrics: 99% accuracy, 98.9% precision, 98% recall, and 98% F1-score. These results strengthen the robustness of the proposed model for high-quality classification, allowing both high positive instance detection rates with low false-positive rates.

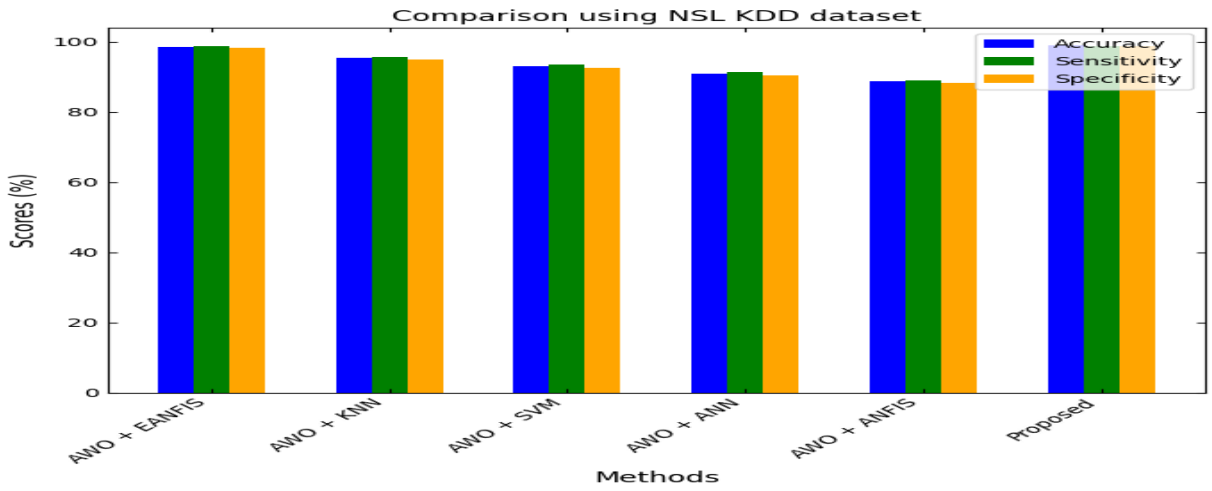

Fig 12. Model comparison using NSL-KDD dataset

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Fig 12 presents a few models, namely: AWO + EANFIS, AWO + KNN, AWO + SVM, AWO + ANN, and AWO + ANFIS, along with the proposed model, in terms of comparative performance metrics for accuracy, sensitivity, and specificity using the NSL-KDD dataset. Performances of some existing models like AWO + EANFIS and AWO + KNN are considerably good, having an accuracy value greater than 95%. However, they definitely fall behind the proposed model with regard to sensitivity and specificity. For instance, AWO + EANFIS records the highest of 98.47%, but its sensitivity and specificity are below this value. This makes the proposed model highly prominent, since all metric values were above 98.5%, indicating its high performance in identifying both attack and normal instances correctly; hence, it proves to be effective for intrusion detection systems. Fig 13 shows a Comparison of the Recall and F1-score of different models on the CICIDS 2017 dataset. Once more, the proposed model shows its excellence since it achieves the highest values of recall (99%) and F1-score (99%). It means that the proposed model is highly capable in identifying the relevant positive instances on one hand, and can balance between precision and recall on the other hand. By comparison, the AWO + EANFIS and AWO + KNN models share the 95% good recall values but with a bit lower F1-score due to the need to balance between precision and recall. Moreover, AWO + SVM and AWO + ANN can be competitive in terms of recall values, but cannot match the F1-score value of the proposed model as well. This makes the proposed model particularly useful for tasks that require as many relevant instances to be returned as possible, with a good balance in the classification performance, such as cybersecurity and fraud detection systems.

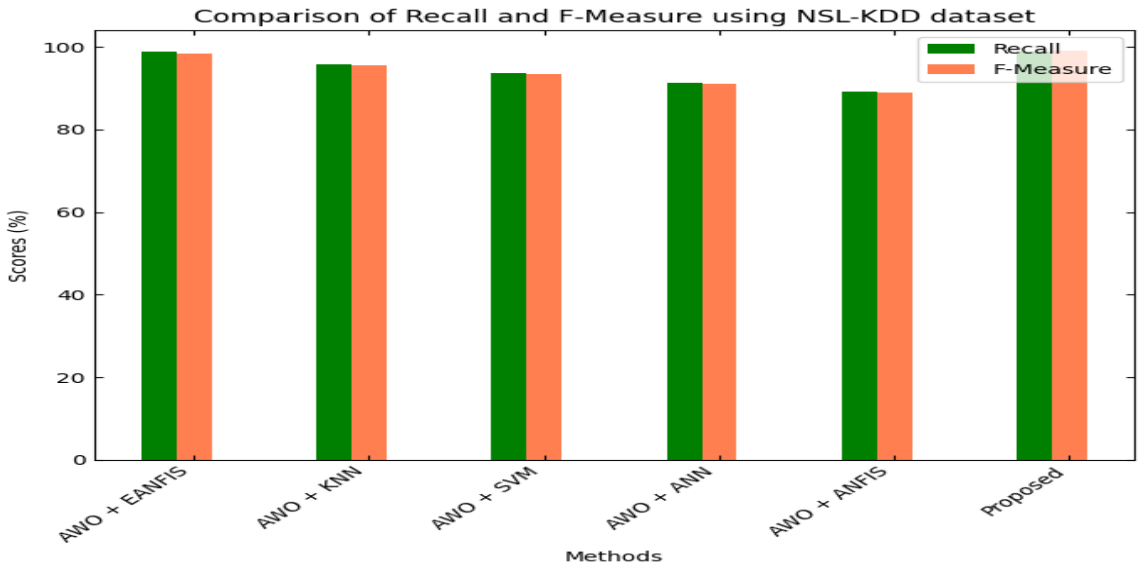

Fig 13. Recall and f1-score comparison using CICIDS 2017 dataset

V. Conclusion

This paper advances two new methodologies to enhance intrusion detection systems and computational processes for optimisation processes, which include BGMNet-for intrusion detection and ShSO for computing batch size. The techniques to be introduced in the present work are designed to cater to the challenges lying in the field of cybersecurity and machine

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

learning by proposing higher-order solutions in terms of detection accuracy and computational efficiency. The Belief Gated Memory Net proposes an intrusion detection state-of-the-art architecture that integrates gated memory mechanisms into a deep learning model. The key novelty of BGMNet is its adaptive capabilities of storing and retrieving important information from previous time steps, thus enhancing the detection of evolving and complex patterns in network traffic. Long-term memory for storage and short-term adaptive gates form part of the working of BGMNet, thereby making it sensitive against real network traffic for any anomalous behavior. Further, Shark Smell Optimization was developed for the batch size computation optimization, which is considered one of the important parameters in deep learning model training. The key contribution of ShSO is related to its efficiency in reducing computational cost associated with the deep learning model training while maintaining or improving the general performance of such models. These results of the experiment showed that ShSO outperforms the traditional optimization techniques in terms of convergence speed and high accuracy, being more effective in large-scale model training with reduced resource consumption. To wrap up, the results of the experiments, conducted on NSL-KDD, CICIDS 2017, and CICIoT 2023 datasets, proved the efficacy of both proposed methods.

REFERENCES

[1] G. Senthilkumar, K. Tamilarasi, and J. Periasamy, "Cloud intrusion detection framework using variational auto encoder Wasserstein generative adversarial network optimized with archerfish hunting optimization algorithm," *Wireless Networks,* vol. 30, pp. 1383-1400, 2024.

[2] Juan Chang, Xiaohong Shen, "Energy-Efficient Barrier Coverage Based on Nodes Alliance for Intrusion Detection in Underwater Sensor Networks," IEEE Sensors Journal, VOL. 22, NO. 4, February 15, 2022.

[3] A. Abid, F. Jemili, and O. Korbaa, "Real-time data fusion for intrusion detection in industrial control systems based on cloud computing and big data techniques," *Cluster Computing,* vol. 27, pp. 2217-2238, 2024.

[4] S. Alzide, "Enhancing Cloud Security through Intrusion Detection: A Comprehensive Study Using the ISOT-CID Dataset," *Journal of Information Technology, Cybersecurity, and Artificial Intelligence,* vol. 1, pp. 39-46, 2024.

[5] N. Sarkar, P. K. Keserwani, and M. C. Govil, "A better and fast cloud intrusion detection system using improved squirrel search algorithm and modified deep belief network," *Cluster Computing,* vol. 27, pp. 1699-1718, 2024.

[6] P. Kaliyaperumal, S. Periyasamy, M. Periyasamy, and A. Alagarsamy, "Harnessing DBSCAN and auto-encoder for hyper intrusion detection in cloud computing," *Bulletin of Electrical Engineering and Informatics,* vol. 13, pp. 3345-3354, 2024.

[7] B. C. Preethi, R. Vasanthi, G. Sugitha, and S. A. Lakshmi, "Intrusion detection and secure data storage in the cloud were recommended by a multiscale deep bidirectional gated recurrent neural network," *Expert Systems with Applications,* vol. 255, p. 124428, 2024.

Received: August 07 2025

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[8] Sibi Amaran1 , Ramalingam Madhan Mohan1 and Rethnaraj Jebakumar2 "Optimal Machine Learning Based Intrusion Detection System in Wireless Sensor Networks for Surveillance Applications," Journal of Mobile Multimedia, Vol. 19 2, 437–450. doi: 10.13052/jmm1550-4646.1924

[9] K. Prabu and P. Sudhakar, "A Comprehensive Survey: Exploring Current Trends and Challenges in Intrusion Detection and Prevention Systems in the Cloud Computing Paradigm," in *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, 2024, pp. 351-358.

[10] E. Silambarasan, R. Suryawanshi, and S. Reshma, "Enhanced cloud security: a novel intrusion detection system using ARSO algorithm and Bi-LSTM classifier," *International Journal of Information Technology,* pp. 1-9, 2024.

[11] C. Fan, J. Cui, H. Jin, H. Zhong, I. Bolodurina, and D. He, "Auto-Updating Intrusion Detection System for Vehicular Network: A Deep Learning Approach Based on Cloud-Edge-Vehicle Collaboration," *IEEE Transactions on Vehicular Technology,* 2024.

[12] Junlin Zhang, "WSNNetwork Node Malicious Intrusion Detection Method Based on Reputation Score", Journal of Cyber Security and Mobility, Vol. 12 1, 55–76. doi: 10.13052/jcsm2245-1439.1213.

[13] V. Saravanan, M. Madiajagan, S. M. Rafee, P. Sanju, T. B. Rehman, and B. Pattanaik, "IoT-based blockchain intrusion detection using optimized recurrent neural network," *Multimedia Tools and Applications,* vol. 83, pp. 31505-31526, 2024.

[14] Ashraf m. etman1, Mohamed s. Abdalzaher ahmeda. emran 2,3, Ahmed Yahya4, And Mostafa Shaaban 2, "A Survey on Machine Learning Techniques in Smart Grids Based on Wireless Sensor Networks", IEEE sensors journal*,vol.13,* pp. 2604-2627, 2025.

[15] B. Mopuru and Y. Pachipala, "Enhanced Intrusion Detection in IoT with a Novel PRBF Kernel and Cloud Integration," *Engineering, Technology & Applied Science Research,* vol. 14, pp. 14988-14993, 2024.

[16] A. Qu, Q. Shen, and G. Ahmadi, "Towards intrusion detection in fog environments using generative adversarial network and long short-term memory network," *Computers & Security,* vol. 145, p. 104004, 2024.

[17] R. K. Ravala, K. B. Polisetty, and S. K. Mishra, "AI Based Feature Selection for Intrusion Detection Classifiers in Cloud of Things," in *2024 1st International Conference on Cognitive, Green and Ubiquitous Computing (IC-CGU)*, 2024, pp. 1-6.

[18] R. Verma, M. Jailia, M. Kumar, and B. Kaliraman, "Deep Neural Network Model for Improved DDoS Attack Detection in Cloud Environments," in *2024 5th International Conference for Emerging Technology (INCET)*, 2024, pp. 1-6.

[19] S. Y. Ali, U. Farooq, L. Anum, N. A. Mian, M. Asim, and T. Alyas, "Securing cloud environments: a Convolutional Neural Network (CNN) approach to intrusion detection system," *Journal of Computing & Biomedical Informatics,* vol. 6, pp. 295-308, 2024.

Received: August 07 2025

Volume 38 No. 9s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[20] S. Biswas and M. S. A. Ansari, "Securing IoT networks in cloud computing environments: a real-time IDS," *The Journal of Supercomputing,* pp. 1-31, 2024.

[21] T. A. Devi and A. Jain, "Enhancing Cloud Security with Deep Learning-Based Intrusion Detection in Cloud Computing Environments," in *2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, 2024, pp. 541-546.

[22] W. a. H. Aljuaid and S. S. Alshamrani, "A deep learning approach for intrusion detection systems in cloud computing environments," *Applied Sciences,* vol. 14, p. 5381, 2024.

[23] J. Zhang, J. D. Peter, A. Shankar, and W. Viriyasitavat, "Public cloud networks oriented deep neural networks for effective intrusion detection in online music education," *Computers and Electrical Engineering,* vol. 115, p. 109095, 2024.

[24] L. Hasimi, D. Zavantis, E. Shakshuki, and A. Yasar, "Cloud computing security and deep learning: An ANN approach," *Procedia Computer Science,* vol. 231, pp. 40-47, 2024.

[25] A. Chaudhari, B. Gohil, and U. P. Rao, "A novel hybrid framework for Cloud Intrusion Detection System using system call sequence analysis," *Cluster Computing,* vol. 27, pp. 3753-3769, 2024/06/01 2024.

[26] H. Chen, Z. Wang, S. Yang, X. Luo, D. He, and S. Chan, "Intrusion detection using synaptic intelligent convolutional neural networks for dynamic Internet of Things environments," *Alexandria Engineering Journal,* vol. 111, pp. 78-91, 2025/01/01/ 2025.

Received: August 07 2025