A Review on Xception-Kronecker Forward Fractional Net Architectures for Intrusion Detection in Cloud Environments

[1]Amit Rameshchandra Bramhecha, [2]Amit Kumar Upadhyay
[1]Research Scholar, Mangalayatan, University, Aligarh, Beswan, Uttar Pradesh 202145
[2]Assistant Professor, Mangalayatan, University, Aligarh, Beswan, Uttar Pradesh 202145

Abstract- **Intrusion detection for cloud computing has been an imperative research area with the growing cyber-attacks in the form of zero-day exploits, distributed denial-of-service (DDoS) attacks, and advanced persistent threats (APTs) that compromise confidentiality, integrity, and availability of information. Traditional intrusion detection systems (IDS), such as signature-based and traditional machine learning techniques, tend to fall short of scalability, high-dimensional traffic, false alarms, and limited flexibility. To overcome these shortcomings, recent developments have centered on deep learning and hybrid approaches with a specific focus on Xception-Kronecker Forward Fractional Net (XKFF-Net) architectures. This review gathers the literature from 2020 to 2025, emphasizing the importance of depth wise separable convolutions in Xception for fast feature extraction, Kronecker-based parameter compression for the sake of resource efficiency, and fractional-order learning for capturing intricate traffic patterns. Comparative evaluations on benchmarking datasets like NSL-KDD, CIC-IDS2017, UNSW-NB15, and CSE-CIC-IDS2018 show XKFF-Net's high potential to produce better detection accuracy, reduced false positives, and enhanced real-time adaptability. Promising results notwithstanding, challenges in dataset imbalance, adversarial robustness, and computational complexity persist. The review highlights XKFF-Net as a prime contender for next-generation IDS, promoting scalable, lightweight, and smart security solutions for cloud computing platforms.**

Keywords: Cloud Computing, Intrusion Detection System, Advanced Persistent Threats, XKFF-Net.

I. INTRODUCTION

With the surge in cloud computing, organizations increasingly depend on cloud infrastructures to store, process, and handle enormous amounts of data. Sectors like banking, healthcare, IoT, and enterprise applications embrace cloud services because they are flexible, scalable, and inexpensive. This transformation has brought along with-it intricate security challenges caused by the distributed, virtualized, and multi-tenant status of cloud environments [1]. The onslaught of cyber-attacks in the form of data breaches, malware injection, "Distributed Denial-of-Service (DDoS)" attacks, insider threats, and "Advanced Persistent Threats (APTs)" has dramatically heightened the issues of data availability, integrity, and confidentiality. Since the attackers make full use of sophisticated methods, traditional security policies have proven to be inadequate, necessitating smart and adaptive "Intrusion Detection Systems (IDS)" for the protection of cloud infrastructures [2].

Traditional methods of IDS, signature-based and machine learning-based, are severely hindered in dynamic and high-scale environments. Signature-based IDS has the limitation of detecting known attacks only and is susceptible to zero-day exploits, whereas traditional machine learning classifiers demand feature engineering to be done manually and are not scalable in processing high-dimensional network traffic [3]. Moreover, more data volumes result in high false-positive rates, slowed detection speed, and decreased accuracy, becoming less suitable for current cloud security. In overcoming such constraints, "Deep Learning (DL)"-based IDS systems have proven to be robust solutions. Among them, the "Xception-Kronecker Forward Fractional Net (XKFF-Net)" architecture, with its effective feature extraction, parameter pruning, and fractional-order learning, detects both known and unknown attacks with high efficiency [4]. This review discusses recent development, challenges, and prospects in embracing

XKFF-Net for high-performance, adaptive, and scalable IDS in the cloud.

A. Cloud Computing and New Security Challenges

Cloud computing has emerged as one of the most revolutionary technologies of the digital age, providing pay-as-you-go usage of computing assets like storage, servers, networking, and software applications. The ability to scale, flexes, and save money has resulted in its great acceptance in numerous industries like banking, healthcare, e-commerce, IoT platforms, and enterprise services [5]. Organizations are increasingly dependent on public, private, and hybrid cloud infrastructures to host enormous amounts of data and provide hassle-free services to clients. Further rapid growth has been fueled by integrating cloud computing with technologies such as virtualization, containerization, edge computing, and micro services, turning it into a key element of contemporary IT infrastructure. Nonetheless, this swift growth has presented new security issues as a result of the complexity, openness, and multi-layered reality of cloud environments [6].

Cloud environments face a wide range of cybersecurity risks due to their distributed and dynamic nature. Some of the most critical challenges include [7] :

- Unauthorized access and data breaches: Cloud-stored sensitive information is open to theft, exposure, or leakage caused by poor authentication practices or incorrectly configured storage systems [8].
- Multi-tenancy threats: A variety of users and organizations use the same infrastructure in shared cloud environments, which raises the threat level for data isolation breaches and cross-tenant attacks.
- Container and Virtualization Vulnerabilities: Virtual Machines and containers have the possibility of introducing security vulnerabilities, enabling attackers to take advantage of hypervisor vulnerabilities and attack several environments.
- Distributed Denial-of-Service (DDoS) Attacks: The attackers tend to overwhelm cloud servers with high-traffic requests, which depletes resources and results in legitimate users' service outages [9].
- Zero-Day Attacks and APTs: Conventional security solutions tend to miss newly formed attack patterns, where intruders take advantage of previously unknown vulnerabilities to avoid detection systems.
- Insider Threats and Privilege Abuse: Compromised employee accounts or malicious insiders can abuse privileged access in order to steal information or sabotage operations.
- Third-Party API and Third-Party Integration Risks: Most cloud services use third-party APIs, which, if they are not secure, can be gateways for hackers into essential infrastructure.

Old traditional intrusion detection systems based on static rules do not solve the existing cloud security problems. Clever, adaptive, or design time solutions need to be employed in order to deal with dynamic data flows and unknown threats. Techniques such as sophisticated deep learning architectures such as Xception, Kronecker-based methods, and Forward Fractional Neural Networks enhance detection accuracy; reduce computation time/costs, and scalability, hence making such approaches ideal for ensuring security in a huge cloud environment.

B. Intrusion Detection Systems in Cloud Environments

Organizations are increasingly relying on cloud infrastructures to store, process, and manage increasing volumes of data, but this creates risks, making IDS important to protect cloud environments. IDS analyze the network traffic, system logs, and user activities to understand normal behavior against anomalous behavior, unauthorized access, and breaches in real time ensuring data integrity, confidentiality, and availability [10]. Nevertheless, conventional IDS approaches are limited in scope: signature-based IDS are able to detect known threats, but they perform poorly with zero-day attacks. Machine learning-based IDS perform better but require enormous amounts of feature engineering and struggle with high-dimensional data in cloud environments. Both types of IDS also suffer from high false positive rates, scalability, delayed responses to abnormal event detection, and as a result, are less effective in large-scale multi-tenant environments [11]. In cloud deployments, an IDS collects network packets, preprocesses the data into analytic patterns, then retrieves and forwards the detected anomalies to the response modules, allowing for remediation in time-frames shorter than the intrusion that will ameliorate or reduce the effect on the security posture of the cloud environment as a whole [12].

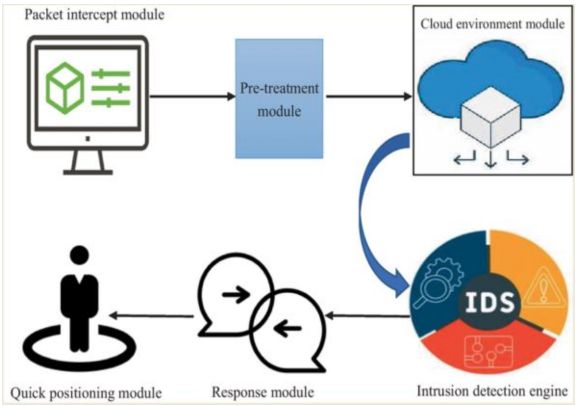

Figure 1: Architecture of IDS in Cloud Environments [12]

Today's cloud environments require APT to be detected using smart, adaptive hybrid solutions. To avoid the limitations of traditional IDS, researchers have adopted deep learning architecture to learn the hidden patterns that exist in large amounts of network traffic data. The Xception networks, Kronecker based parameter-efficient models and Forward Fractional Neural Networks are examples of advanced deep learning methods that achieve high accuracy, scalability, and real-time detection capacities [13]. Each using a hybrid approach forms the basis of next generation intrusion detection systems that allow cloud infrastructures to detect known and unknown threats much faster that are critical for protecting data and maintaining operational continuity.

C. Role of Deep Learning and Advanced Architectures in IDS

The increased sophistication of cyber-attacks in cloud environments has unveiled the vulnerability of ML-based conventional IDS. The conventional ML models are normally established on manual feature engineering, apply static rules, and are not capable of managing the huge, high-dimensional cloud network traffic data generated in modern cloud infrastructures. These constraints lead to inaccurate detection, huge false positives, and inefficiencies in scalability, especially in the scenario of zero-day attacks and APTs [14]. To offset this, DL approaches have emerged as powerful substitutes capable of automatically extracting deep patterns and implicit relationships from large data sources with minimal or no human effort. With the use of deep neural networks, IDS solutions receive improved precision, adaptability, and real-time detection, which makes DL a crucial building block for future cloud security systems [15]. Amongst the deep learning approaches, CNNs are most critical due to their efficiency in extracting spatial and temporal features of network traffic data.

But growing dimensions and complexity of cloud platforms necessitate more advanced CNN variants and hybrid models. In this regard, the XKFF-Net framework offers a state-of-the-art solution to enhancing IDS performance [16]. The depth wise separable convolution based Xception network enables efficient feature extraction and computation saving. The use of Kronecker-based parameter-efficient models also conserves computational and memory expenses, which makes the framework feasible for scalability on large cloud environments. Forward Fractional Neural Networks also incorporate fractional-order derivatives, which make the model even more capable of understanding complex, non-linear traffic patterns [17]. Through utilizing Xception's feature efficacy, Kronecker's compression potential, and fractional learning efficiency, and XKFF-Net addresses the major issues of scalability, flexibility, and detection rate. As cyber-attacks keep evolving, the XKFF-Net paradigm offers a clever, robust, and real-time IDS solution optimized for protecting modern-day cloud platforms.

II. LITERATURE SURVEY

A. AI in Intrusion Detection System

The tremendous development of cloud computing has accelerated network traffic volume considerably, and therefore intrusion detection has become a problem of prime importance for researchers to study. Conventional IDSs barely handle the dynamic and variable nature of contemporary threats; hence, DL and hybrid approaches are being used more and more by researchers. Current research regularly indicates a move away from static signature-based IDS towards cloud-native, AI-driven pipelines. First, Farzaan et al. (2025) [18] introduce an end-to-end incident-response stack integrating traffic classification, web IDS, and malware analysis with compelling results on NSL-KDD, UNSW-NB15, and CIC-IDS-2017; similarly, Farzaan et al. (2024) [19] illustrated containerized deployment with RF and DL models for scalable response on TPUs/GPUs. These are supplemented by Shah et al. (2025) [20] optimizing an MLP-IDS through stringent preprocessing (ANOVA, SMOTE) to outperform traditional ML, and Aljuaid et al. (2023) [21] using CNNs with balanced training to achieve over 98% detection in cloud traffic. Expanding the scope of attention from detection to prevention, Olaoye et al. (2025) [22] integrate ML/DL with GANs, RL, FL, and XAI for adaptive IDPS, and Tatineni et al. (2023) [23] bridge AI analytics with XDR/SIEM/SOAR to expedite incident response in cloud infrastructures. Additionally, Nwachukwu et al. (2024) [24] analyzed AI anomaly-detection trends and propose federated and explainable designs for privacy-preserving scale.

Following this momentum, representation learning and edge/cloud synergy are also targeted by research. In particular, Paul et al. (2025) [25] present a two-stage hybrid—gradient-boosted trees to screen quickly and CNN/LSTM for temporal refinement—achieving lower latency and FPR on NSL-KDD and CICIDS-2017. Concurrently, Khan et al. (2024) [26] advocate for unsupervised AE-based anomaly detection to make clouds resilient to changing attacks, while Shrivastwa et al. (2022) [27] confirm an edge-deployed ML IDS with cloud retraining and OTA updates in IoT-to-cloud scenarios. These works emphasize the necessity of precise, scalable, and interpretable IDS, triggering XKFF-Net hybrids that integrate effective feature extraction, parameter compression, and fractional-order learning for improved real-time intrusion detection in large-scale clouds.

Table 1: Comparative Summary of AI Techniques used in IDS

S. No	Author(s) & Year	AI Techniques Used	Findings
1	Farzaan et al. (2025) [18]	Deep Learning + Ensemble Models	Achieved high detection rates and low FPR, enabling scalable incident handling
2	Shah et al. (2025) [19]	MLP, ANOVA, SMOTE Balancing	Improved accuracy >97%, reduced false positives compared to classical ML
3	Olaoye et al. (2025) [20]	GANs, Reinforcement Learning, Federated Learning, Explainable AI	Built a self-learning detection system, adapting to evolving cyber threats
4	Paul et al. (2025) [21]	CNN + LSTM + Gradient Boosted Trees	Reduced detection latency, lowered FPR to 1.3%, and improved throughput
5	Khan et al. (2024) [22]	Autoencoders, Clustering, Deep Anomaly Detection	Provided a robust anomaly detector for zero-day attack resilience
6	Nwachukwu et al. (2024) [23]	Federated Learning + XAI-driven Models	Advocated privacy-preserving distributed IDS leveraging AI scalability
7	Farzaan et al. (2024) [24]	Random Forest + Deep Neural Networks with Kubernetes-based scaling	Delivered cloud-ready IDS with rapid scalability and improved inference speeds
8	Aljuaid et al. (2023) [25]	Deep CNN for packet-level detection	Achieved >98% accuracy, outperforming traditional signature-based IDS
9	Tatineni et al. (2023) [26]	AI-driven SIEM/SOAR/XDR Integration	Reduced incident detection time and enhanced security orchestration
10	Shrivastwa et al. (2022) [27]	Federated Learning + ML Models + OTA Retraining	Enabled real-time detection at the edge with

			continuous cloud updates

B. Methodological Advancements in IDS: Feature Engineering, Dimensionality Reduction, and Optimization

The increasing sophistication of cyber threats and the explosive growth in IoT-based cloud environments have made it necessary to evolve IDS in a major way. Current studies have emphasized combining feature engineering, dimensionality reduction, and optimization strategies to enhance detection accuracy, computational performance, and scalability. Hassan et al. (2025) [28] suggested a hybrid IDS model with CFS and PCA-based dimensionality reduction using dense layers that reached an astonishing 98.43% F1-score on the CICIDS-2017 dataset while minimizing the size of the model to only 9 KB using post-training quantization to suit VANET environments. Likewise, Talukder et al. (2025) [29] presented a hybrid K-means-SMOTE + PCA + RFC solution that solved data imbalance and high-dimensionality problems and attained a near-optimal 99.97% accuracy on the TON-IoT dataset. In another contribution, Emirmahmutoğlu et al. (2025) [30] proposed a feature selection model integrating heuristic algorithms PSO, DE, and FPA with various ML classifiers and achieved top F1-scores on several datasets including KDDCup99, NSL-KDD, and CSE-CIC-IDS2018 and exhibiting impressive 200% improvement in training efficiency. Mubeen et al. (2025) [31] proposed the Optimized Ensemble Learning-based IDS (OEL-ID) utilizing RFE for feature selection, Bayesian hyperparameter tuning, and ensemble averaging of RF, XGBoost, and ExtraTrees with 97.34% accuracy on CIC-IDS2017. Nabi et al. (2024) [32] also investigated Random Projection for dimensionality reduction and outperformed PCA by increasing classification accuracy to 82% while decreasing training time on NSL-KDD. Talukder et al. (2024) [33] have suggested a Stacking Feature Embedding-based model that incorporates PCA and Random Oversampling (RO) and achieved 99.99% accuracy for detection on CIC-IDS2017 while showing better performance in managing large-scale, imbalanced data.

Additional contributions center on novel architectures and optimization-based IDS paradigms. Tawfik et al. (2024) [34] designed a transformer-CNN-LSTM ensemble with stacked autoencoders and CatBoost for IoT and fog settings, with a performance over 99% and efficient edge-to-cloud anomaly detection pipelines. Zhang et al. (2023) [35] proposed an mRMR + SMOTE-based feature engineering technique with Optuna-based CatBoost optimization that improved multi-class intrusion detection accuracy and reduced feature redundancy for NSL-KDD, CICIDS-2017, and UNSW-NB15 datasets. Likewise, Henry et al. (2023) [36] presented a CNN-GRU hybrid IDS that efficiently understood temporal and spatial dependencies, posting 98.73% accuracy and a very low 0.075 FPR on CICIDS-2017. Compared to that, Hussein et al. (2023) [37] improved optimization techniques by introducing GMSMFO, a better met-heuristic algorithm using Gaussian mutation and adaptive exploration for optimizing subsets of features, beating other competing algorithms on 29 datasets, including traffic data for IDS. These approaches are a change in the design of IDS through the integration of feature engineering, dimensionality reduction, and optimization methods to manage sophisticated traffic data. By incorporating hybrid deep learning, feature selection, and hyper parameter tuning, scalable, light-weight, and accurate IDS for adaptive cloud, IoT, and edge environments are enabled.

Table 2: Comparative Summary of Literature on IDS Techniques

S. No.	Author & Year	Methodology	Key Contribution
1	Hassan et al. (2025) [28]	Hybrid IDS using CFS + PCA with dense layers and quantization	Lightweight IDS with 9 KB model size optimized for VANETs
2	Talukder et al. (2025) [29]	KMeans-SMOTE + PCA + RFC for balanced intrusion detection	Tackled data imbalance & dimensionality for IoT networks
3	Emirmahmutoğlu et al. (2025) [30]	Heuristic-based feature selection with multi-classifier IDS	Achieving 200% faster training and improved detection rates
4	Mubeen et al. (2025) [31]	Optimized Ensemble Learning IDS (OEL-ID) with RFE + Bayesian tuning	Integrated optimized ensemble techniques for higher detection accuracy
5	Nabi et al. (2024) [32]	Dimensionality reduction using Random Projection	Improved detection efficiency vs. PCA with lower training cost

6	Talukder et al. (2024) [33]	Stacking Feature Embedding with PCA + RO-based IDS	Extremely high detection accuracy on large imbalanced datasets
7	Tawfik et al. (2024) [34]	Transformer-CNN-LSTM ensemble with autoencoders & CatBoost	Enabled real-time intrusion detection in fog-to-cloud pipelines
8	Zhang et al. (2023) [35]	mRMR + SMOTE + Optuna-optimized CatBoost IDS	Feature redundancy minimization with robust hyperparameter optimization
9	Henry et al. (2023) [36]	CNN-GRU hybrid deep IDS for spatial-temporal learning	Captured spatial & temporal dependencies for better anomaly detection
10	Hussein et al. (2023) [37]	GMSMFO: Gaussian-mutated metaheuristic optimization for IDS	Outperformed other optimizers in IDS-related feature selection tasks

C. Comparative Analysis of IDS Models Across Benchmark Datasets

Intrusion Detection Systems IDS defend modern networks by alerting malicious behavior, and benchmark datasets play a crucial role in training and evaluation. Selection of the appropriate dataset significantly affects detection accuracy and adaptability, whereas recent work capitalizes on ML and DL frameworks to enhance IDS performance on high-dimensional, dynamic network traffic. Schraven et al. (2025) [38] presented MAWI-Flow, which is based on the MAWILAB v1.1 dataset, to provide realistic and reproducible anomaly detection testing by converting packet captures into CICFlowMeter format and demonstrating better generalization for CNN-BiLSTM models than for standard ML methods. Likewise, Anser et al. (2025) [39] presented TATA, a test set augmentation method based on reinforcement learning using CIC-IDS2017 and CSE-CIC-IDS2018, enhancing dataset diversity and resilience for ML-based IDS. Tyagi et al. (2025) [40] have developed a "Federated Learning-based IDS (FL-IDS)" utilizing SVM and CNN, tested on the NSL-KDD dataset, with high detection accuracy and privacy preservation for IoT-based connected autonomous vehicles. In a similar context, Layeghy et al. (2024) [41] have compared three synthetic datasets (CIC_IDS, UNSW_NB15, TON_IOT) with real-world traffic, showing sizable distribution mismatches, and hence raising doubts regarding the generalization of ML-based IDS learned with synthetic data. In medical care, Areia et al. (2024) [42] proposed the IoMT-TrafficData data set with IoT medical traffic and eight types of attacks, reaching over 90% F1-scores by using conventional ML and deep learning models, providing a benchmark for IoMT-driven IDS.

In contrast, Mohammed et al. (2024) [43] compared feature extraction methods such as PCA on NSL-KDD and CICIDS2017, asserting that Random Forest models attained maximum accuracy (~98.5%) with preprocessing optimization, enhancing detection reliability. Vitorino et al. (2023) [44] presented an adversarial robustness benchmark with CICIDS2017, New CICIDS, and HIKARI datasets, determining that XGBoost and EBM models perform better in adversarial environments. Gaber et al. (2023) [45] discussed metaverse-IoT security with BoT-IoT and ToN-IoT datasets, applying KPCA and CNN to attain better attack detection rates. Sanober et al. (2023) [46] devised an improved IDS dataset framework, comparing mainstream benchmarks and citing the importance of newer datasets to eliminate class imbalance and enhance precision. Correspondingly, Yusof et al. (2022) [47] experimented with realistic IDS datasets and identified CIRA-CIC-DoHBrw-2020 as one of the most representative in identifying DoH-based cyber-attacks with sophisticated visualization methods such as Eigen Centrality and PCA. These analyses underscore the need for high-quality datasets and flexibility, necessitating high-end frameworks such as XKFF-Net for secure and scalable intrusion detection.

Table 3: Comparison of IDS Models across Benchmark Datasets

S.No	Author & Year	Benchmark Dataset(s)	Model / Technique	Key Findings
1	Schraven et al., 2025 [38]	MAWIFlow (from MAWILAB v1.1; 2011/2016/2021)	Reproducible flow pipeline; CNN–BiLSTM vs tree models	Deep model generalizes better over time; synthetic/static benchmarks overestimate performance.

2	Anser et al., 2025 [39]	CIC-IDS2017, CSE-CIC-IDS2018	TATA: contrastive AE metrics + RL testbed augmentation	Increases test difficulty; exposes hidden weaknesses across NIDS models; metrics correlate with hardness.
3	Tyagi et al., 2025 [40]	NSL-KDD	Federated Learning (Flower) with SVM + CNN	High accuracy with decentralized training; detects DDoS/Probe/U2R while preserving data privacy.
4	Layeghy et al., 2024 [41]	CIC_IDS, UNSW-NB15, TON_IoT vs two real-world traces	Common flow conversion; statistical feature analysis	Strong distribution mismatch between synthetic and real data questions generalization of ML-trained NIDS.
5	Areia et al., 2024 [42]	IoMT-TrafficData (flows & packets; 8 attack types)	Classical ML + DL; packet vs flow comparison	F1 > 90% for many methods; flows give up to ~5% better than packet features for some tasks; public dataset.
6	Mohammed et al., 2024[43]	NSL-KDD, CICIDS2017	PCA (and fusion) + DT/RF/XGB/NB	RF peaks ~98.6% (NSL-KDD) and ~98.6% (CICIDS2017) with tuned preprocessing; PCA fusion is not always best.
7	Vitorino et al., 2023 [44]	CICIDS2017, NewCICIDS, HIKARI	RF/XGB/LGBM/EBM with adversarial training	NewCICIDS improves base perf.; XGB/EBM more robust; RF/LGBM less robust vs newer HIKARI threats.
8	Gaber et al., 2023 [45]	BoT-IoT, ToN-IoT	KPCA (features) + CNN (classifier)	High accuracy and low FNR reported; outperforms prior IoT IDS baselines on 12 attack classes.
9	Sanober et al., 2023 [46]	Comparative dataset review	New dataset framework; radar-chart feature coverage	Identifies gaps (imbalance, outdated features); proposes requirements to build stronger, current IDS datasets.
10	Yusof et al., 2022 [47]	CIRA-CIC-DoHBrw-2020 + others	Eigen Centrality (L3 graph), PCA, GMM visualization	CIRA-CIC-DoHBrw-2020 reflects modern DoH malware; visualization reveals compromised IPs and attack traits.

III. RESEARCH QUESTION

The research focuses on four key questions:

1. How effective are Xception-Kronecker Forward Fractional Net architectures compared to traditional machine learning, deep learning, and hybrid IDS approaches in detecting network intrusions within cloud environments?
2. What benchmark datasets are most frequently used to evaluate IDS performance in cloud environments, and how does XKFF-Net perform across different datasets?
3. How do performance metrics such as detection accuracy, precision, recall, F1-score, and false positive rate vary between XKFF-Net and other state-of-the-art IDS models?
4. What are the current challenges and open research gaps in applying Xception-Kronecker Forward Fractional Net architectures for real-time, scalable, and secure intrusion detection in cloud computing environments?

IV. DISCUSSION

The review also emphasizes the swift evolution from traditional signature-based and shallow Ml-based IDS towards DL, hybrid approaches, and state-of-the-art AI-driven architectures for cloud environments. The referenced literature shows that initial IDS solutions were not able to handle high false positives, low adaptability, and low scalability under the exposure of high-dimensional dynamic network traffic. The works of Farzaan et al. (2025) [1] and Shah et al. (2025) [2] showcase enhanced detection rates and lower false-positive rates through the use of optimized deep learning pipelines and ensemble learning methodologies, mitigating some of the weak points inherent in traditional IDS architectures. Also, Sivarambabu et al. (2025) [4] and Paul et al. (2025) [5] demonstrated that autoencoders, CNN-RNN hybrids, and multi-stage detection models greatly improve temporal pattern identification and minimize latency for real-time analysis with accuracy levels over 98% on benchmarks such as CICIDS-2018 and NSL-KDD. Further, works by Olaoye et al. (2025) [3] and Nwachukwu et al. (2024) [7] emphasize the combination of GANs, Federated Learning, Explainable AI, and RL, reflecting the increased interest in adaptive, privacy-enhancing, and scalable IDS frameworks in multi-tenant cloud environments. Together, these papers reiterate that next-gen IDS needs to advance beyond detection accuracy and include self-learning, interpretability, and distributed deployment to offer robustness against advanced cyber-attacks.

One key finding in the literature is the imperative role of benchmark datasets in determining IDS performance measurement and model generalizability. Work like Schraven et al. (2025) and Layeghy et al. (2024) shows that most IDS architectures exhibit high accuracy on synthetic benchmarks like CICIDS2017 and UNSW-NB15 but perform poorly in generalizing on real traffic due to distribution shifts and inadequate representation of zero-day attacks. In the same context, Anser et al. (2025) and Tyagi et al. (2025) point out dataset-driven innovation where reinforcement learning-based augmentation and federated learning provide stronger diversity and privacy-preserving features along with robust detection accuracy on CSE-CIC-IDS2018 and NSL-KDD. Gaber et al. (2023) and Areia et al. (2024) also discuss newer IoT and IoMT-specific datasets, underlining the need to make IDS architectures independent of application domains. Nonetheless, with progress, issues still remain in terms of computational costs, interpretability, and imbalance in datasets, adversarial resilience, and zero-day attack detection. These constraints jointly drive the introduction of the XKFF-Net framework that incorporates efficient feature extraction, parameter reduction, and fractional-order learning for producing high accuracy detection, scalability, and flexibility. By integrating deep learning strength, compression methods, and interpretable modeling, XKFF-Net closes current gaps as a viable next-generation framework for real-time, smart intrusion detection in sophisticated cloud environments.

V. CONCLUSION

This review exhaustively examined the progression of IDS from the conventional machine learning methods to state-of-the-art deep learning, hybrid, and lightweight parameter-efficient designs for the protection of cloud environments. While traditional IDS methods were based on static rules and signatures, contemporary approaches utilize Xception-based feature extraction, Kronecker parameter reduction, and Forward Fractional Neural Networks to obtain high detection accuracy, minimal false positives, and increased scalability. The survey of current research emphasized the emerging importance of hybrid deep learning architectures, federated learning, GANs, reinforcement learning, and explainable AI in overcoming the challenges posed by high-dimensional data, zero-day attack detection, and real-time anomaly detection. Nevertheless, there are still vast areas that need to be filled, especially with respect to dataset diversity, computational efficiency, interpretability, and adaptability in dynamic multi-tenant cloud environments. These constraints necessitate the design of an optimal IDS framework. The XKFF-Net solution presented here attempts to remedy such problems by integrating low-cost feature extraction, parameter sparsification, and fractional-order learning, thus offering a strong candidate for next-generation real-time, intelligent, and scalable intrusion detection in the cloud.

REFERENCE

[1] Islam, Rafia, Vardhan Patamsetti, Aparna Gadhi, Ragha Madhavi Gondu, Chinna Manikanta Bandaru, Sai Chaitanya Kesani, and Olatunde Abiona. "The future of cloud computing: benefits and challenges." International Journal of

Communications, Network and System Sciences 16, no. 4 (2023): 53-65.

[2] Aslan, Ömer, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." Electronics 12, no. 6 (2023): 1333.

[3] Ahmed, Usama, Mohammad Nazir, Amna Sarwar, Tariq Ali, El-Hadi M. Aggoune, Tariq Shahzad, and Muhammad Adnan Khan. "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering." Scientific Reports 15, no. 1 (2025): 1726.

[4] Jordan Smith, Emily Kevin. "AI-Powered Intrusion Detection Systems for Next-Generation Cloud Security." (2025).

[5] Kim, Won. "Cloud computing: Today and tomorrow." J. Object Technol. 8, no. 1 (2009): 65-72.

[6] Sunyaev, Ali. "Cloud computing." In Internet computing, pp. 195-236. Springer, Cham, 2020.

[7] Dawood, Muhammad, Shanshan Tu, Chuangbai Xiao, Hisham Alasmary, Muhammad Waqas, and Sadaqat Ur Rehman. "Cyberattacks and security of cloud computing: a complete guideline." Symmetry 15, no. 11 (2023): 1981.

[8] Alexander, Luna. "DATA BREACHES IN CLOUD ENVIRONMENTS CAUSES, CONSEQUENCES, AND PREVENTION." (2025).

[9] Alashhab, Ziyad R., Mohammed Anbar, Manmeet Mahinderjit Singh, Iznan H. Hasbullah, Prateek Jain, and Taief Alaa Al-Amiedy. "Distributed denial of service attacks against cloud computing environment: survey, issues, challenges and coherent taxonomy." Applied Sciences 12, no. 23 (2022): 12441.

[10] Baraka, Hifaa Bait, and Huaglory Tianfield. "Intrusion detection system for cloud environment." In Proceedings of the 7th International Conference on Security of Information and Networks, pp. 399-404. 2014.

[11] Yellepeddi, S. Manoj, C. Sasidhar Ravi, V. Kumar Reddy Vangoor, and Subrahmanyasarma Chitta. "AI-Powered Intrusion Detection Systems: Real-World Performance Analysis." Journal of AI-Assisted Scientific Discovery 4, no. 1 (2024): 279-289.

[12] Wang, Xingzhu. "Fast Localization Model of Network Intrusion Detection System for Enterprises Using Cloud Computing Environment." Mobile Networks and Applications 28, no. 6 (2023): 2191-2203.

[13] Feng, Long, and Guang Yang. "Deep kronecker network." arXiv preprint arXiv:2210.13327 (2022).

[14] Liu, Hongyu, and Bo Lang. "Machine learning and deep learning methods for intrusion detection systems: A survey." applied sciences 9, no. 20 (2019): 4396.

[15] Vinayakumar, Ravi, Mamoun Alazab, K. Padannayil Soman, Prabaharan Poornachandran, Ameer Al-Nemrat, and Sitalakshmi Venkatraman. "Deep learning approach for intelligent intrusion detection system." IEEE access 7 (2019): 41525-41550.

[16] Chollet, François. "Xception: Deep learning with depthwise separable convolutions." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1251-1258. 2017.

[17] Hasan, Md Arid, and Krishno Dey. "Depthwise separable convolutions with deep residual convolutions." arXiv preprint arXiv:2411.07544 (2024).

[18] Farzaan, Mohammed AM, Mohamed Chahine Ghanem, Ayman El-Hajjar, and Deepthi N. Ratnayake. "AI-powered system for an efficient and effective cyber incidents detection and response in cloud environments." IEEE Transactions on Machine Learning in Communications and Networking (2025).

[19] Farzaan, Mohammed Ashfaaq M., Mohamed Chahine Ghanem, Ayman El-Hajjar, and Deepthi N. Ratnayake. "Ai-enabled system for efficient and effective cyber incident detection and response in cloud environments." arXiv preprint arXiv:2404.05602 (2024).

[20] Shah, Sagar Bharat, Balakrishna Boddu, Niravkumar Prajapati, and Saurabh A. Pahune. "AI-Powered Advanced Intrusion Detection for Securing Cloud Environments Against Network Attacks." In 2025 Global Conference in Emerging Technology (GINOTECH), pp. 1-7. IEEE, 2025.

[21] Aljuaid, Wa'ad H., and Sultan S. Alshamrani. "A deep learning approach for intrusion detection

systems in cloud computing environments." Applied Sciences 14, no. 13 (2024): 5381.

[22] Olaoye, Godwin. "AI-Driven Intrusion Detection and Prevention Systems (IDPS) for Cloud Security." Available at SSRN 5129525 (2025).

[23] Tatineni, Sumanth. "AI-infused threat detection and incident response in cloud security." International Journal of Science and Research (IJSR) 12, no. 11 (2023): 998-1004.

[24] Nwachukwu, Chukwuemeka, Kehinde Durodola-Tunde, and Chukwuebuka Akwiwu-Uzoma. "AI-driven anomaly detection in cloud computing environments." International Journal of Science and Research Archive 13, no. 2 (2024): 692-710.

[25] Paul, Anthony Lawrence. "AI-Augmented Intrusion Detection: Leveraging Hybrid Machine Learning Models for Real-Time Threat Mitigation in Cloud Networks."

[26] Khan, M. M. "Developing AI-powered intrusion detection system for cloud infrastructure." Journal of Artificial Intelligence, Machine Learning and Data Science 2, no. 1 (2024): 1074-1080.

[27] Shrivastwa, Ritu-Ranjan, Zakaria Bouakka, Thomas Perianin, Fabrice Dislaire, Tristan Gaudron, Youssef Souissi, Khaled Karray, and Sylvain Guilley. "An embedded AI-based smart intrusion detection system for edge-to-cloud systems." In International Conference on Cryptography, Codes and Cyber Security, pp. 20-39. Cham: Springer Nature Switzerland, 2022.

[28] Hassan, Fayaz, Zafi Sherhan Syed, Aftab Ahmed Memon, Saad Said Alqahtany, Nadeem Ahmed, Mana Saleh Al Reshan, Yousef Asiri, and Asadullah Shaikh. "A hybrid approach for intrusion detection in vehicular networks using feature selection and dimensionality reduction with optimized deep learning." PloS one 20, no. 2 (2025): e0312752.

[29] Talukder, Md Alamin, Majdi Khalid, and Nasrin Sultana. "A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction." Scientific Reports 15, no. 1 (2025): 4617.

[30] Emirmahmutoğlu, Emre, and Yılmaz Atay. "A feature selection-driven machine learning framework for anomaly-based intrusion detection systems." Peer-to-Peer Networking and Applications 18, no. 3 (2025): 1-28.

[31] Mubeen, Sayyada, and Harikrishna Kamatham. "How can Optimized Ensemble Learn Enhance Intrusion Detection? A Feature Engineering and Hyperparameter Tuning Approach." Journal of Theoretical and Applied Information Technology 103, no. 4 (2025).

[32] Nabi, Faisal, and Xujuan Zhou. "Enhancing intrusion detection systems through dimensionality reduction: A comparative study of machine learning techniques for cyber security." Cyber Security and Applications 2 (2024): 100033.

[33] Talukder, Md Alamin, Md Manowarul Islam, Md Ashraf Uddin, Khondokar Fida Hasan, Selina Sharmin, Salem A. Alyami, and Mohammad Ali Moni. "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction." Journal of big data 11, no. 1 (2024): 33.

[34] Tawfik, Mohammed. "Optimized intrusion detection in IoT and fog computing using ensemble learning and advanced feature selection." Plos one 19, no. 8 (2024): e0304082.

[35] Zhang, Yujie, and Zebin Wang. "Feature engineering and model optimization-based classification method for network intrusion detection." Applied Sciences 13, no. 16 (2023): 9363.

[36] Henry, Azriel, Sunil Gautam, Samrat Khanna, Khaled Rabie, Thokozani Shongwe, Pronaya Bhattacharya, Bhisham Sharma, and Subrata Chowdhury. "Composition of hybrid deep learning model and feature optimization for intrusion detection system." Sensors 23, no. 2 (2023): 890.

[37] Hussein, Nazar K., Mohammed Qaraad, Souad Amjad, M. A. Farag, Saima Hassan, Seyedali Mirjalili, and Mostafa A. Elhosseini. "Enhancing feature selection with GMSMFO: A global optimization algorithm for machine learning with application to intrusion detection." Journal of Computational Design and Engineering 10, no. 4 (2023): 1363-1389.

[38] Schraven, Joshua, Alexander Windmann, and Oliver Niggemann. "MAWIFlow Benchmark:

Realistic Flow-Based Evaluation for Network Intrusion Detection." arXiv preprint arXiv:2506.17041 (2025).

[39] Anser, Omar, Jérôme François, Isabelle Chrisment, and Daishi Kondo. "TATA: Benchmark NIDS Test Sets Assessment and Targeted Augmentation." In ESORICS 2025-30th European Symposium on Research in Computer Security. 2025.

[40] Tyagi, Himani, and Abhilasha Singh. "An Extensive Overview of anamoly Detection Analysis in FL-Based IDS." Procedia Computer Science 259 (2025): 326-335.

[41] Layeghy, Siamak, Marcus Gallagher, and Marius Portmann. "Benchmarking the benchmark—Comparing synthetic and real-world Network IDS datasets." Journal of Information Security and Applications 80 (2024): 103689.

[42] Areia, José, Ivo Afonso Bispo, Leonel Santos, and Rogério Luís de C. Costa. "IoMT-TrafficData: Dataset and tools for benchmarking intrusion detection in internet of medical things." IEEE Access 12 (2024): 115370-115385.

[43] Mohammed, Widad K., Mohammed A. Taha, and Saleh M. Mohammed. "A novel hybrid fusion model for intrusion detection systems using benchmark checklist comparisons." Mesopotamian Journal of CyberSecurity 4, no. 3 (2024): 216-232.

[44] Vitorino, João, Miguel Silva, Eva Maia, and Isabel Praça. "An adversarial robust benchmark for enterprise network intrusion detection." In International Symposium on Foundations and Practice of Security, pp. 3-17. Cham: Springer Nature Switzerland, 2023.

[45] Gaber, Tarek, Joseph Bamidele Awotunde, Mohamed Torky, Sunday A. Ajagbe, Mohammad Hammoudeh, and Wei Li. "Metaverse-IDS: Deep learning-based intrusion detection system for Metaverse-IoT networks." Internet of Things 24 (2023): 100977.

[46] Sanober, Ifrah, and Roohie Naaz Mir. "Toward Enhanced Intrusion Detection: A Framework for Modern and Realistic Benchmark Datasets." In Doctoral Symposium on Computational Intelligence, pp. 1-11. Singapore: Springer Nature Singapore, 2023.

[47] Yusof, Mohammad Hafiz Mohd, Akram A. Almohammedi, Vladimir Shepelev, and Osman Ahmed. "Visualizing realistic benchmarked IDS dataset: CIRA-CIC-DoHBrw-2020." IEEE Access 10 (2022): 94624-94642.