Communications & Networks Connect
ISSN: 3105-1421
2025, Article ID. 2025.0010, Cite as: https://doi.org/10.69709/CNC.2025.112097

SCIFINITI PUBLISHING

Research Article

OPEN ACCESS

A Unified Snort–OSSEC Hybrid Intrusion Detection Framework for Cloud Security

Idris Olanrewaju Ibraheem✉,* **Abdulrauf Uthman Tosho**✉

Department of Computer Science, Faculty of Computing, Engineering and Technology, Al-Hikmah University, Adewole Estate, Ilorin PMB 1601, Nigeria

Article History

Submitted: August 03, 2025 Accepted: November 16, 2025 Published: December 08, 2025

Abstract

The increasing adoption of cloud computing has led to improvements in cost-efficiency and operational effectiveness; however, it has also resulted in heightened security vulnerabilities due to its distributed and multi-tenant architecture. The contribution of this study lies in enhancing cloud security through the development of a hybrid intrusion detection system (IDS) that integrates Snort (N-IDS) and OSSEC (H-IDS) to achieve cross-layer alert correlation. Unlike standalone deployments or other deep learning models that are computationally intensive, the framework proposed is an open-source framework that is interpretable and also deployable in real-world environments. The experimental evaluation within a cloud testbed shows that the hybrid IDS was able to achieve 97.1% accuracy, a 94.1% detection rate, and a false alarm rate of only 0.2%, which performed better than Snort-only and OSSEC-only systems. Case-based simulations further demonstrated that hybrid correlation not only enhances detection but also reduces false positives and provides improved forensic trails, particularly in scenarios involving port scanning, brute-force login attempts, and user-to-root exploits. When compared with previous IDS studies, the system achieved competitive accuracy while maintaining efficiency and transparency. Although evaluated in a limited-scale environment, this study provides a practical foundation for developing adaptive, scalable, and prevention-oriented frameworks in cloud security.

Keywords:

cloud security; hybrid IDS; Snort; OSSEC; network security; Intrusion Detection System (IDS)

1. Introduction

Cloud computing has changed modern information technology as it has enabled scalable, flexible, and cost-effective access to computing resources and storage. From personal applications and other enterprise services, the adoption of cloud computing has grown across industries. Although this shift has brought about increased security concerns, due to cloud infrastructure being a frequent target of several cyberattacks that include denial-of-service, privilege escalation, and data exfiltration [1]. The protection of cloud environments requires intrusion detection systems (IDS) that can detect and act fast to this malicious activity before the dire effect on the service integrity or confidentiality.

Some research conducted over the past decade explored network-based IDS (N-IDS) and host-based IDS (H-IDS) as primary defense mechanisms. Network-based IDS (N-IDS) such as Snort excel at monitoring network traffic for suspicious patterns; however, they often fail to detect host-level anomalies that bypass perimeter defenses. However, OSSEC, which is an H-IDS solution, provides system-level monitoring although it lacks visibility in broader traffic flows. As it relies just on either results that are limited to host activities coverage and the likelihood of false positives or undetected attacks occurrence [2]. Furthermore, most previous IDS implementations have focused primarily on the detection of known signatures, often exhibiting reduced effectiveness against unknown or zero-day threats [3].

* **Corresponding Author:**
Idris Olanrewaju Ibraheem, Department of Computer Science, Faculty of Computing, Engineering and Technology, Al-Hikmah University, Adewole Estate, Ilorin PMB 1601, Nigeria, ioibraheem@alhikmah.edu.ng

To address this research gap, there is a need to develop integrated IDS frameworks that combine host- and network-level perspectives to achieve effective detection capabilities while minimizing false alarms. Some recent studies have attempted hybrid IDS designs, although most of them focus on simulations, while others were not validated adequately in real-world cloud testbeds [4]. To be precise, some studies demonstrated how the integration of Snort and OSSEC, two widely adopted open-source IDS tools, can be used within a hybrid framework that empirically validates improved detection performance.

This study addressed the gaps with the design, implementation, and evaluation a hybrid Snort–OSSEC IDS framework practically in a cloud computing environment. The system uses both signature-based and anomaly-based techniques to detect a wide range of attacks, leveraging cross-layer alert correlation to improve accuracy and reduce misclassification. Unlike existing models, the framework went through empirical validation by carrying out simulated attack scenarios that include port scanning, DoS, brute-force, and U2R executed against an Ubuntu-based OwnCloud testbed.

1.1. Research Objectives

The objectives of this study are as follows:

1. To design and implement a hybrid IDS framework that integrates Snort and OSSEC for cloud environments.
2. To simulate attack scenarios and evaluate the detection performance.
3. To compare the performance of Snort-only, OSSEC-only, and the hybrid IDS for accuracy, detection rate, and false alarm rate.
4. To benchmark the proposed framework against previous IDS studies to show its novelty and practical contribution.

1.2. Scope of the Study

This study was conducted on a virtualized Ubuntu-based cloud testbed running OwnCloud, Apache, and MariaDB. The hybrid intrusion detection system was implemented using two widely adopted open-source tools: Snort for network-level monitoring and OSSEC for host-level monitoring. Four attack categories, port scanning, denial-of-service (DoS), brute-force, and user-to-root (U2R), are the basis of the assessment, which represent common threats in cloud environments. The focus of this study was on improving detection performance and reducing false alarms through cross-layer correlation. The need for scalability to large multi-tenant deployments and integration with prevention mechanisms was outside the present scope and is recommended for future research.

2. Literature Review

The literature on intrusion detection in cloud computing has seen immense growth, which reflects the need to balance scalability with security. Intrusion detection systems (IDS) have been widely studied, although there are still challenges in addressing unknown threats, reducing false alarms, and ensuring real-time performance in environments that are of a distributed nature. This section reviews some of the existing approaches carried out on cloud service models, common attack vectors, and hybrid IDS designs, and identifies the limitations of the previous methods in relation to the proposed framework.

2.1. Cloud Services and Security Challenges

Cloud services are typically categorized into Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The users are exposed to VM-to-VM attacks and hypervisor vulnerabilities through IaaS, Insecure API and multi-tenancy issues are mostly from PaaS, while confidentiality and compliance issues are mostly the concerns from SaaS based deployments. Previous studies outlined these risks, but often the emphasis is always on governance and policy over the integration of IDS mechanisms [5]. More recent studies predict sustained growth in cloud service adoption, but give little or no attention to the implementation of IDS within these contexts [6]. It became necessary to address these gaps by developing and deploying adaptable intrusion detection solutions that span service layers.

2.2. Attack Vectors in Cloud Environments

Cloud infrastructures face various attack vectors. Side-channel exploits, which are virtual-machine-based attacks, demonstrate how easily privilege escalation can occur across tenants. User-to-root (U2R) exploits have been studied with classifiers such as Naïve Bayes and ANN, even though detecting these exploits remains difficult given their low frequency [7]. The prevalence of DoS and DDoS threats continues to rise, with distributed detection frameworks often burdened by computational overhead [1]. Datasets with Backdoors and adversarial attack vectors represent growing risks for IDS robustness, which shows the need for anomaly-based detection that can withstand the evolving threats [3,8].

2025, Vol. 2, Article ID. 2025.0010
https://doi.org/10.69709/CNC.2025.112097

There have been Hybrid IDS approaches that attempt to integrate N-IDS and H-IDS techniques. The early designs showed great promise but could not be validated at the host level, and in some cases were tested only on simulated datasets [9]. In a study by [10], a two-phase hybrid IDS was proposed that improved detection rates; however, the work suffers from high false-positive rates. A recent survey on AI-driven models reported very high accuracy on benchmark datasets, and some hybrid CNN–RNN designs have achieved accuracy levels exceeding 98% [11]. However, these systems often compromise interpretability and require high computation, which limits deployment in resource-constrained cloud environments [12].

Recent and advanced studies emphasize the use of adaptive and federated approaches. [1], in their research introduced a hybrid IDS with the combination of XGBoost and deep learning components on various datasets. This model improved accuracy but also raised concerns about generalizability. The study by [4] complemented transformer-based models with graph features, which achieved almost perfect accuracy, but the implementation wasn't validated in a real-world environment. In [7], a deep learning IDS for IoT networks was introduced; however, its ability to perform optimally and effectively in cloud environments remains uncertain. These studies highlight the importance of adaptive, explainable, and scalable IDS for detecting unknown attacks and reducing false alarms, but they also indicate a persistent gap in practical, open-source deployments. From this review, three main gaps were noted:

1. Most IDS frameworks place more emphasis on either known signature detection or anomaly-based detection. The combination of both techniques is rarely explored, even though it is effective in a real cloud testbed.
2. Previous hybrid systems lack empirical validation of cross-layer integration that consists of network and host to reduce false positives.
3. Recent AI-based IDS studies tend to achieve high accuracy but often compromise deployability and interpretability in cost-sensitive environments.

This study addresses these gaps with the implementation and validation of a Snort–OSSEC hybrid IDS with correlated alerting, tested against multiple attack classes, and the performance evaluated based on metrics such as accuracy, detection rate, and false alarm rate.

3. Materials and Methods

3.1. Study Aim and Design

The primary aim of this study was to design and evaluate a hybrid intrusion detection system (IDS) that integrates Snort, a network-based IDS, and OSSEC, a host-based IDS, to enhance cloud security. A quasi-experimental testbed design was used, which involves controlled attack simulations against a cloud-based environment. The performance of three configurations Snort-only, OSSEC-only, and Snort–OSSEC hybrid was also compared to determine the relative advantages of the hybridization technique employed.

Figure 1 illustrates how Snort N-IDS and OSSEC H-IDS operate independently and then correlate alerts through a combined analysis engine, depicted as the central controller. It shows the flow of data from network traffic and system logs to detection and correlation.

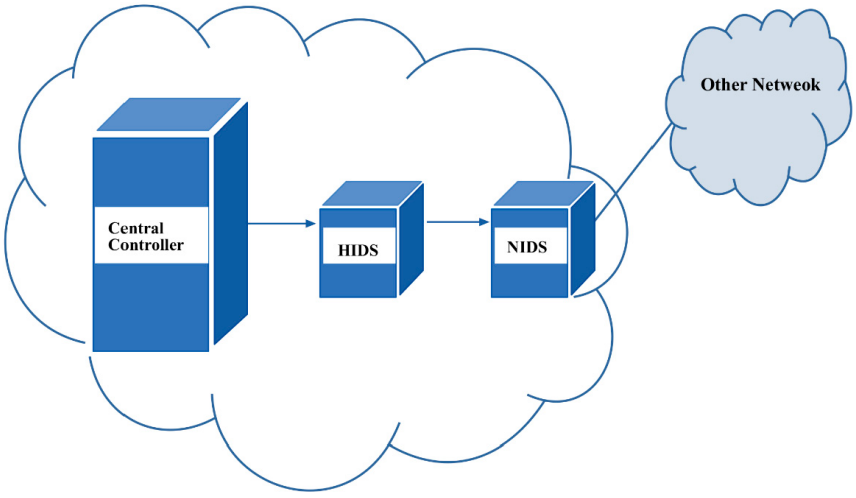

Figure 1: Architecture of the proposed Snort–OSSEC hybrid IDS framework.

3.2. Study Setting

The study was conducted in an isolated laboratory environment that was configured to replicate a realistic cloud service. An Ubuntu 20.04 LTS server was deployed as the primary cloud platform, running OwnCloud to simulate cloud storage and collaboration services. Supporting services included MariaDB for database management and the Apache HTTP Server for web hosting. This setup provided a clear multi-tier cloud architecture for testing intrusion detection mechanisms under real-world conditions.

3.3. Materials and Tools

The following are the materials used in this study that include both software and hardware:

1. IDS Tools: Snort version 2.9.17 for packet inspection, OSSEC version 3.7.0 for host log and integrity monitoring.
2. Traffic Capture and Analysis: Wireshark version 3.4.7.
3. Attack Tools: Nmap for port scanning, Hping3 for DoS traffic generation, Hydra for brute-force login attempts, and Metasploit for U2R privilege escalation.
4. Dataset Source: The primary dataset used was generated from simulated attacks on the isolated testbed, which consists of 14,072 labeled connections.
5. Hardware Environment: Physical and virtualized PC running Ubuntu as the server and Attacker PC on VMware ESXi with 8-core CPU, 32 GB RAM, and 100 GB allocated storage.

Figure 2 shows the workflow: network traffic is first filtered by protocol type (TCP, UDP, ICMP, HTTP/FTP), then passed to a processing queue for analysis against a pattern database by the detection engine. All matches generate alerts that are logged and trigger notifications, while regular traffic is archived. This layered process of detection and reporting shows the integration of Snort (N-IDS) and OSSEC (H-IDS) for cross-validation and improved accuracy.

The attack simulation structure is detailed in Figure 3, which shows the complete experimental process.

3.3.1. Attack Simulation Process

Controlled simulations were conducted to validate the system's detection capabilities across multiple attack categories. Open-source security tools were employed to generate attacks, ensuring reproducibility. Nmap was used for port scanning by probing open ports and identifying vulnerable services; Hping3 generated TCP/ICMP floods targeting the OwnCloud server to simulate Denial-of-Service (DoS) attacks; Hydra attempted repeated password logins against FTP services for brute-force attacks; and Metasploit modules were utilized to simulate privilege escalation on the Ubuntu server for user-to-root exploits.

Each attack was executed against the testbed with corresponding Snort rules and OSSEC alerts monitored in real time. By including both frequent (port scans, DoS) and rare (U2R) categories, the review covered a wide range of threat scenarios.

The testbed was deployed on an Ubuntu environment, which hosts the OwnCloud server with Apache and MariaDB, as shown in Figure 3. Snort was configured as a network intrusion detection system (N-IDS) to monitor packet-level traffic, while OSSEC was configured as a host intrusion detection system (H-IDS) to log and monitor system integrity. An attacker machine was configured to generate malicious traffic using Nmap, Hping3, Hydra, and Metasploit, while Wireshark was used for packet capturing and analysis. This setup enabled controlled evaluation of the hybrid IDS under real-world cloud attack scenarios.

This diagram, as shown in Figure 4, indicates the process by which attack simulations, such as port scanning, denial-of-service (DoS), brute-force login, and user-to-root (U2R), are launched from the attacker machine against the cloud testbed. Snort monitors network traffic, while OSSEC analyzes system-level logs. The alerts triggered from both sources are forwarded to the hybrid correlation module, where a cross-validation technique is in place to improve detection accuracy and reduce false alarms.

In this study, 'unknown threats' refer to attacks that are not included in the initial Snort signature sets or the predefined OSSEC rules. Detection was enabled through anomaly-based mechanisms: Snort leveraged preprocessors to identify unusual traffic behaviors, such as abnormal packet sizes and protocol misuse, while OSSEC used integrity checks and system log correlation to capture deviations from baseline user activities.

This dual-layer anomaly detection ensured that threats absent from signature databases could still be flagged as suspicious, supporting claims of "unknown" detection capability.

2025, Vol. 2, Article ID. 2025.0010
https://doi.org/10.69709/CNC.2025.112097

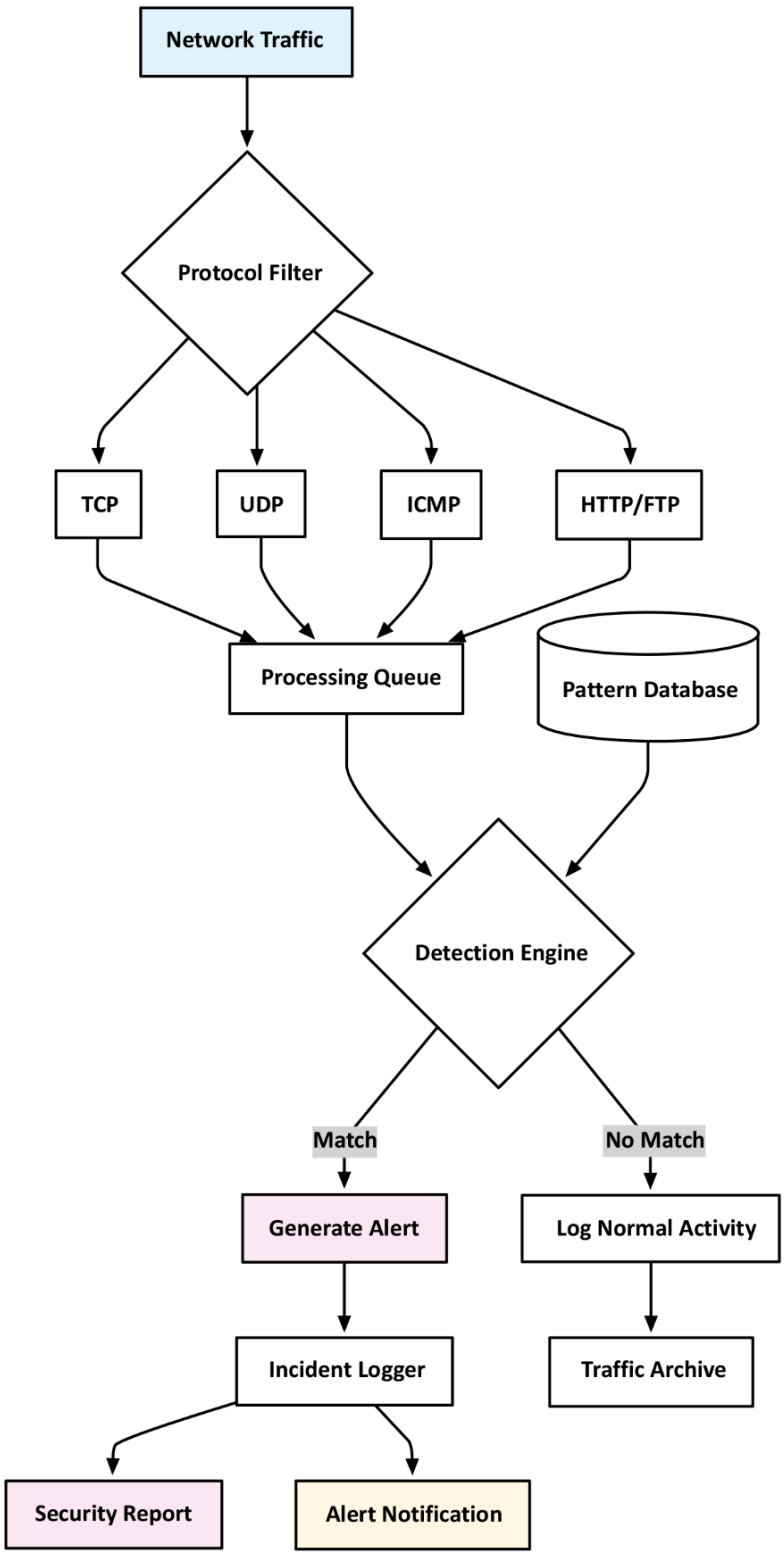

Figure 2: Comprehensive flowchart of the proposed hybrid IDS model.

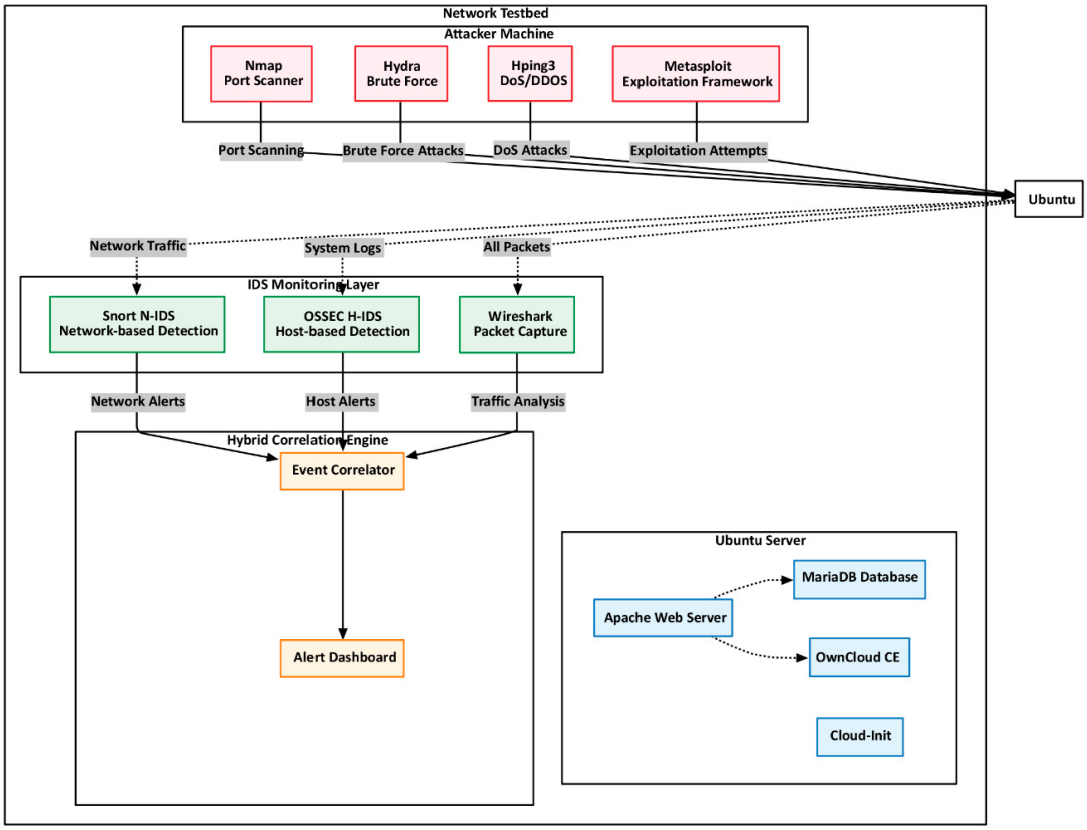

Figure 3: Experimental testbed setup for hybrid IDS evaluation.

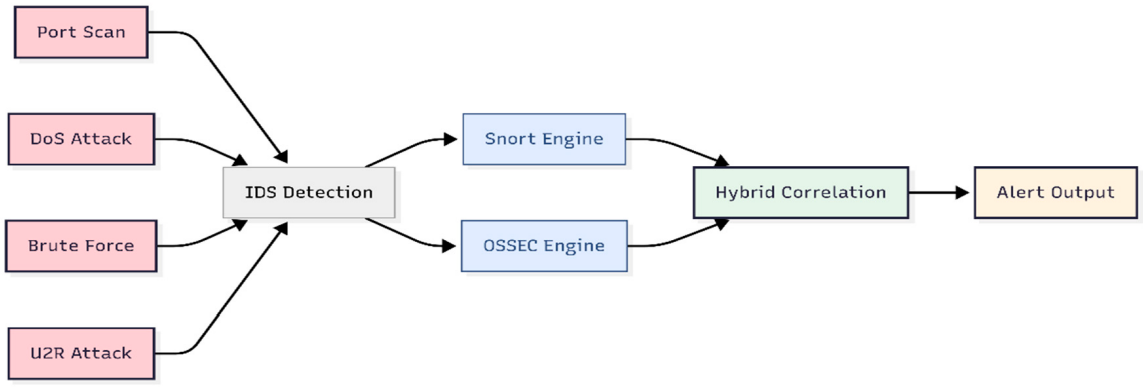

Figure 4: Integrated network and host security workflow.

3.4. Data Collection Procedures

The benign traffic was initially generated by cloud services during regular user activities. While Wireshark captures network-layer packets, OSSEC simultaneously monitors host-level system events and file integrity, providing comprehensive visibility across both network and host environments. Upon completion of baseline profiling, controlled attacks were carried out against the testbed using the tools listed above. Every attack scenario was repeated several times for consistency. Captured traffic and logs were stored in packet capture (pcap) and syslog formats for preprocessing. All experiments were carried out in an isolated laboratory testbed that had no connection to external networks. By doing that, it ensured that simulated attacks posed no risk to production systems or third-party infrastructure.

2025, Vol. 2, Article ID. 2025.0010
https://doi.org/10.69709/CNC.2025.112097

3.5. Data Preprocessing and Feature Extraction

Initially, 31 attributes were recorded from the Snort logs; after normalization and feature selection, only 26 were retained. These attributes include protocol type, source and destination ports, connection duration, TCP flags, packet size, and byte counts. Additionally, the OSSEC host-based IDS (H-IDS) contributed features such as failed login attempts, file integrity modifications, and unauthorized root access events. All the features were then presented in a tabular form to create a structured dataset that is suitable for classification as shown in Table 1.

Table 1: Extracted features from hybrid IDS logs.

Category	Features
Protocol & Connection	Protocol type (TCP/UDP/ICMP/FTP), source IP, destination IP, source port, destination port, packet length, connection duration
Network Behavior	TCP flags (SYN, ACK, FIN, RST), number of bytes sent/received, packets per connection, abnormal fragmentation
Service Indicators	FTP login attempts, number of concurrent sessions, and failed authentication events
Host Activities	File integrity changes, unauthorized root access attempts, and log modification frequency
Traffic Context	Time interval between packets, abnormal ICMP echo requests, and unexpected UDP connections

3.5.1. Features Before Normalization (31 Features)

Duration, Protocol_type, Service, Flag, Src_bytes, Dst_bytes, Land, Wrong_fragment, Urgent, Hot, Num_failed_logins, Logged_in, Num_compromised, Root_shell, Su_attempted, Num_root, Num_file_creations, Num_shells, Num_access_files, Num_outbound_cmds, Is_host_login, Is_guest_login, Count, Srv_count, Serror_rate, Srv_serror_rate, Rerror_rate, Srv_rerror_rate, Same_srv_rate, Diff_srv_rate, Srv_diff_host_rate

3.5.2. Features After Normalization (26 Features)

Duration, Protocol_type, Service, Flag, Src_bytes, Dst_bytes, Wrong_fragment, Urgent, Num_failed_logins, Logged_in, Num_compromised, Root_shell, Su_attempted, Num_root, Num_file_creations, Num_shells, Num_access_files, Is_guest_login, Count, Srv_count, Serror_rate, Srv_serror_rate, Rerror_rate, Srv_rerror_rate, Same_srv_rate, Diff_srv_rate

3.6. Interventions and Comparisons

Three system configurations were tested:

1. Snort-only (N-IDS)—network-level detection only.
2. OSSEC-only (H-IDS)—host-level detection only.
3. Hybrid Snort–OSSEC IDS—correlated alerts across host and network layers.

Each configuration underwent an evaluation phase based on identical attack scenarios, allowing for a comparative analysis of accuracy, detection rate, and false alarm rate.

3.7. Classifier Justification: Naïve Bayes

The justification for the selection of the Naïve Bayes classifier for the evaluation of the detection performance is due to its suitability for categorical and discrete data that are derived from Snort and OSSEC logs. Its advantages include:

1. Computational efficiency: suitable for real-time IDS applications with large datasets.
2. Noise tolerance: Its effectiveness in handling imperfect or incomplete network traffic data.
3. Transparency: its ability to provide interpretable probability outputs, enhancing explainability in cloud security.

While deep learning methods have achieved higher accuracy in some IDS studies, they usually require substantial computational resources and lack interpretability. The lightweight and explainable nature of Naïve Bayes makes it appropriate for practical, cost-sensitive cloud deployments.

3.8. Evaluation Metrics

The Naïve Bayes classifier was used to evaluate detection performance based on its efficiency, noise tolerance, and interpretability [12]. Performance metrics were calculated from confusion matrices using the following formulas (Equations (1)–(3)):

i. Accuracy

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

ii. Detection Rate

$$DR = \frac{TP}{TP+FN} \quad (2)$$

iii. False Alarm Rate

$$FAR = \frac{FP}{TN+FP} \quad (3)$$

4. Results

4.1. Experimental Setup in Relation to Methods

As outlined in Section 3.4, the evaluation was conducted in an Ubuntu OwnCloud testbed where four attack scenarios, port scanning, DoS, brute-force, and U2R, were simulated using Nmap, Hping3, Hydra, and Metasploit. The three IDS configurations described in Section 3.6 Interventions and Comparisons were tested separately: Snort-only, OSSEC-only, and the hybrid Snort–OSSEC framework. The primary dataset used for evaluation comprised 14,072 labeled connections generated during these experiments.

4.2. Classifier Evaluation: Confusion Matrix

Using the dataset described in Section 3.5 and the Naïve Bayes classifier introduced in Section 3.7, the classifier's performance was first evaluated in terms of its confusion matrix. Table 2 presents the distribution of classification outcomes across normal and anomalous traffic. Out of a total of 7,446 normal connections, 7,430 were correctly classified, while only 16 were misclassified as anomalies. For the anomalous connections, out of 6626 connections, 6239 were correctly detected, while 387 were misclassified as usual.

4.3. Classifier Evaluation: Performance Metrics

From the confusion matrix, the standard performance measures (accuracy, detection rate, false alarm rate, precision, F-measure, MCC, ROC area, PRC area) were calculated using the formulas defined in Section 3.8. The results are shown in Table 3.

Table 2: Confusion matrix of the naïve bayes classifier.

Actual Class	Predicted Normal	Predicted Anomaly
Normal	True Negative (TN) = 7430	False Positive (FP) = 16
Anomaly	False Negative (FN) = 387	True Positive (TP) = 6239

Table 3: Performance of the naïve bayes classifier on the class of connections.

Class	TP Rate	FP Rate	Precision	F-Measure	MCC	ROC Area	PRC Area
Anomaly	0.998	0.058	0.950	0.974	0.944	0.993	0.987
Normal	0.942	0.002	0.997	0.969	0.944	0.994	0.996
Weighted Avg.	0.971	0.032	0.973	0.972	0.944	0.994	0.991

These results demonstrate the classifier's ability to discriminate effectively between normal and anomalous connections, with ROC and PRC areas above 0.99, confirming robustness.

4.4. Class and Protocol-Based Analysis

To further analyze the distribution of detection, classification outcomes were visualized.

Figure 5, the Connection Class Chart, illustrates the classification split between normal and anomalous traffic, showing a strong bias toward correct predictions in both categories.

Additionally, Figure 6 presents the traffic analysis by protocol (TCP, UDP, ICMP, HTTP/FTP), illustrating the system's coverage of diverse network activities. The illustration shows that the IDS successfully handled protocol heterogeneity, validating the importance of protocol-aware detection in hybrid frameworks.

4.5. Standalone IDS Performance

The performance of Snort and OSSEC when deployed independently was assessed. As detailed in Section 3.6, both IDSs were evaluated using the same traffic dataset. Table 4 summarizes the results.

2025, Vol. 2, Article ID. 2025.0010
https://doi.org/10.69709/CNC.2025.112097

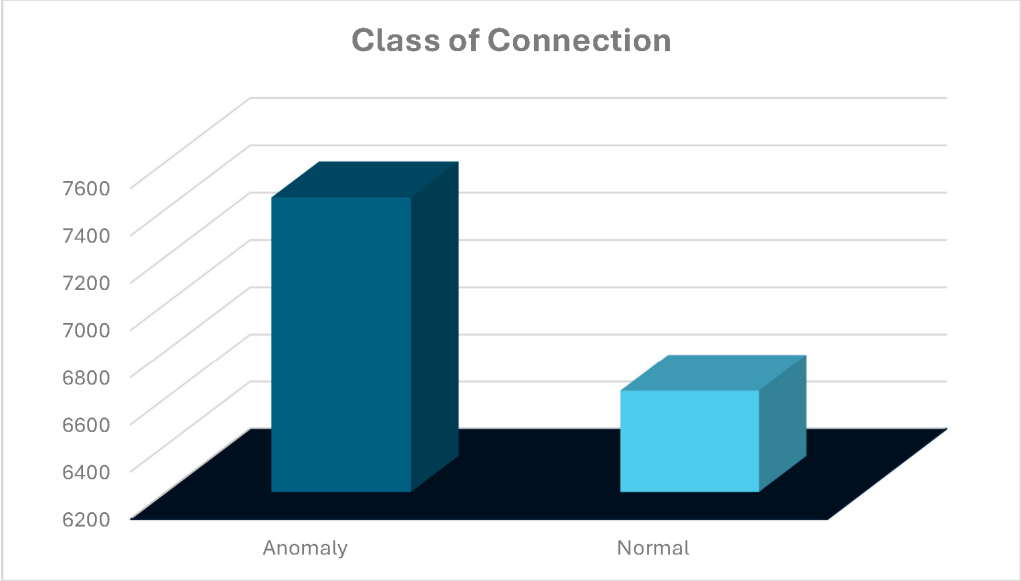

Figure 5: Distribution of network traffic by connection class.

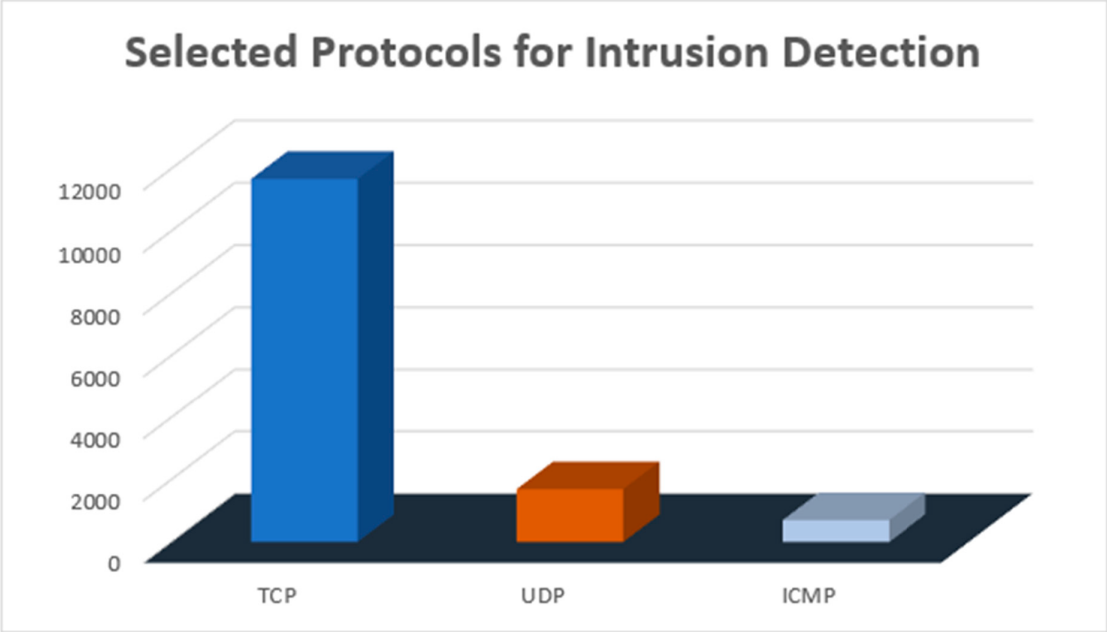

Figure 6: Frequency analysis of network protocols in intrusion detection.

4.6. Hybrid IDS Performance

When Snort and OSSEC were integrated, the hybrid IDS achieved significantly higher performance. Table 5 and Figures 7 and 8 compare the hybrid IDS to the standalone systems.

Table 5 compares Snort-only, OSSEC-only, and the proposed hybrid IDS in terms of accuracy, detection rate, and false alarm rate. While the standalone systems performed well individually, each exhibited critical blind spots: Snort failed to detect host-level exploits, whereas OSSEC was less effective against reconnaissance attacks. The hybrid IDS overcame these gaps, achieving the highest accuracy (97.1%) and detection rate (94.1%) while reducing the false alarm rate to just 0.2%. These results confirm the advantage of cross-layer correlation in delivering a more reliable intrusion detection solution for cloud environments.

Table 4: Standalone IDS performance.

System	Accuracy	Detection Rate	False Alarm Rate	Observations
Snort (N-IDS)	94.6%	91.2%	1.3%	Effective for port scans and DoS, but missed host-level exploits.
OSSEC (H-IDS)	92.8%	89.7%	1.7%	Strong for brute-force and privilege escalation, but missed reconnaissance attacks.

Table 5: Hybrid IDS vs standalone systems.

System	Accuracy	Detection Rate	False Alarm Rate	Key Benefits
Snort-only	94.6%	91.2%	1.3%	Missed host-level attacks
OSSEC-only	92.8%	89.7%	1.7%	Missed early reconnaissance
Hybrid (Snort + OSSEC)	97.1%	94.1%	0.2%	Cross-validation reduced false positives and expanded coverage

The grouped bar chart, as shown in Figure 7, compares Snort-only, OSSEC-only, and the hybrid IDS across accuracy, detection rate, and false alarm rate. The hybrid IDS clearly outperformed standalone systems, achieving the highest accuracy (97.1%) and detection rate (94.1%), while reducing the false alarm rate to just 0.2%.

The line chart, as shown in Figure 8, illustrates the trend of performance metrics across IDS configurations. While both Snort and OSSEC performed well individually, the hybrid IDS consistently achieved superior results across all metrics, confirming the advantage of cross-layer correlation.

The hybrid IDS clearly outperforms the standalone systems, achieving both higher detection rates and significantly lower false alarms.

4.7. Comparative Analysis with Previous Studies

Finally, the performance of the hybrid IDS was benchmarked against prior studies.

The bar chart in Figure 9 compares the performance of the proposed hybrid IDS with five representative studies [1,4,10,11]. While previous work achieved strong accuracy, false alarm rates remained relatively high, ranging from 0.9% to 2.1%. By contrast, the proposed hybrid IDS achieved a balanced performance with 97.1% accuracy and a 0.2% false alarm rate, demonstrating superior efficiency and reliability in a real-world testbed environment.

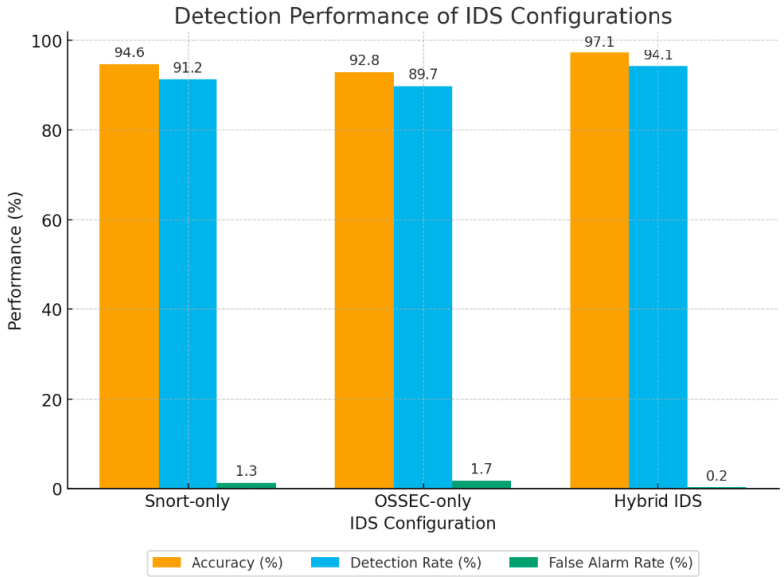

Figure 7: Detection performance of IDS configurations.

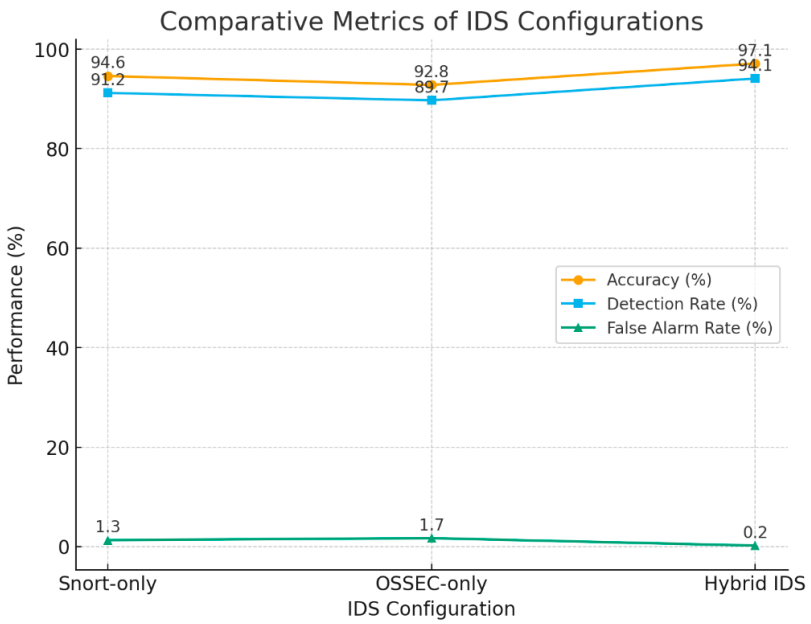

Figure 8: Comparative metrics of IDS configurations.

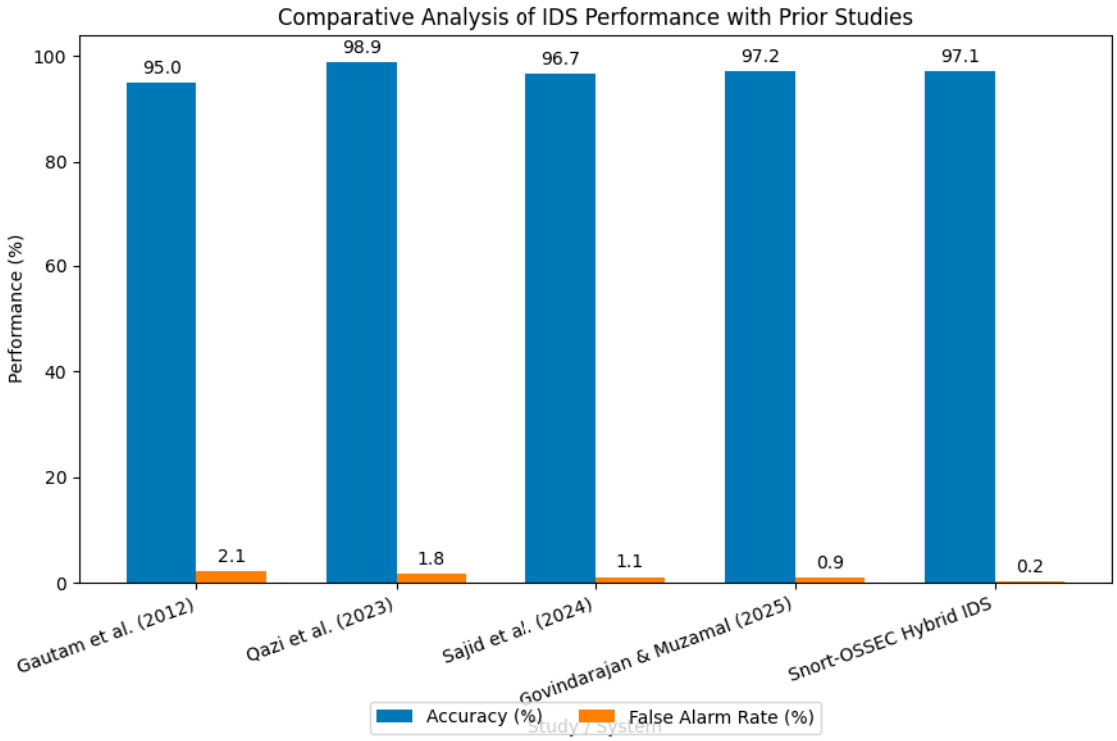

Figure 9: Comparative analysis of IDS performance with previous studies.

5. Discussion

The results of this study demonstrate the effectiveness of hybridizing Snort (N-IDS) and OSSEC (H-IDS) to enhance intrusion detection in cloud environments. The Naïve Bayes classifier came out strong, achieving a higher classification performance as shown in Table 3 with ROC and PRC areas above 0.99, which confirms its reliability

in differentiating between normal and anomalous connections. The confusion matrix, as shown in Table 2, further illustrates balanced performance across classes, with reduced false positives (16) and a small number of false negatives (387). This demonstrates the classifier's effectiveness in practical detection scenarios.

Figures 7 and 8 provide additional insight into classification behavior and traffic diversity. The class of connection distribution (Figure 7) visually confirms the system's high accuracy across both normal and anomalous classes, complementing the confusion matrix and performance metrics. Likewise, the protocol-based chart in Figure 6 shows that attacks spanned TCP, UDP, ICMP, and HTTP/FTP traffic. This confirms the hybrid framework's ability to address protocol heterogeneity and reiterates the need for cross-layer monitoring.

When evaluated as standalone systems, Snort and OSSEC each displayed strengths, but also critical gaps highlighted in Table 6 [1,3,4,7,9–14]. Snort performed well on reconnaissance and volumetric attacks, while OSSEC detected brute-force and privilege-escalation attempts more effectively. However, both suffered from blind spots when used in isolation. The integration of the two systems into the hybrid framework closed these gaps, achieving a significantly higher accuracy of 97.1% and detection rate of 94.1%, with an impressively low false alarm rate of 0.2%. The outcome indicates the importance of cross-layer alert correlation in reducing false alarms and enhancing reliability.

Table 6: Comparative analysis of the snort–OSSEC hybrid IDS framework against existing literature.

Study	Approach	Limitations	Improvement in This Work
Mazzariello et al. (2010) [8]	Integrated N-IDS in open-source cloud	No host-level validation; limited scope	Adds OSSEC (H-IDS) with Snort for cross-layer monitoring
Gupta (2015) [9]	Hybrid IDS (KFsensor + FlowMatrix)	Improved detection but many false positives	Cross-layer correlation reduces false positives significantly
Pandeeswari & Kumar (2016) [13]	ANN + Naïve Bayes for anomaly detection	Struggled with rare U2R/R2L attacks	Hybrid Snort–OSSEC validated on U2R and brute-force scenarios
Sajid et al. (2024) [1]	Hybrid ML + deep learning IDS across multiple datasets	High accuracy, but generalizability and computational cost concerns	Lightweight NB classifier in hybrid IDS balances accuracy with efficiency
Govindarajan & Muzamal (2025) [4]	Graph-based features + transformers, near 99.9% accuracy	Extremely resource-intensive; no testbed validation	Demonstrates cost-effective, real-world validation using open-source tools
Khan et al. (2023) [12]	Hybrid deep learning IDS (RNN-GRU for IoT)	IoT-specific focus, limited cloud applicability	Tailored for cloud context with Snort + OSSEC hybrid
Qazi et al. (2023) [10]	CNN + RNN hybrid IDS (HDLNIDS) on CICIDS2018	Very high accuracy (>98%) but black-box, lacks interpretability	Hybrid IDS provides explainability and transparent probabilistic outputs
Kimanzi et al. (2024) [11]	Review of DL-based IDS algorithms	Highlights high accuracy but lack of interpretability	Responds with an interpretable, open-source hybrid IDS framework
Boukela et al. (2023) [3]	Active learning IDS with DNN + KNN	Detects unknown attacks, but not tested in cloud settings	Hybrid IDS validated on unknown threats in a practical cloud testbed
Belarbi et al. (2023) [14]	Federated deep learning IDS for IoT networks	Improves F1 but complex deployment and data-sharing overheads	Lightweight hybrid model suitable for single-cloud, cost-sensitive environments
Snort-OSSEC Hybrid IDS (2025)	Hybrid Snort–OSSEC IDS with cross-layer correlation	Limited to small-scale testbed; focused on 4 attack types; lacks IPS capability	Validated in real cloud testbed; achieved 97.1% accuracy, 94.1% DR, 0.2% FAR; interpretable and cost-effective

5.1. Case-Based Evaluation of Hybrid Correlation

Case-specific examples from the attack simulations in Section 3.4 highlight the advantages of the hybrid framework. In the case of a port scan, Snort detected a TCP SYN scan with medium confidence while OSSEC logged multiple failed login attempts; together, the correlated alerts confirmed malicious intent and eliminated what would have been a false positive in Snort-only mode. During the brute-force login attempt, OSSEC detected multiple failed FTP login attempts, which Snort corroborated by identifying abnormal TCP connection patterns, thereby distinguishing the incident from ordinary user error. For a user-to-root (U2R) exploit, OSSEC detected privilege escalation while Snort traced suspicious pre-attack reconnaissance, producing a more comprehensive forensic trail. Results from the cases suggest that hybrid correlation improves detection rates, validates alerts, reduces false positives, and enhances forensic analysis.

Comparative analysis with previous studies, as shown in Figure 9 further positions this work within the state of the art. Deep learning-based systems, such as those proposed by [1,4], achieved high accuracy but are computationally expensive and often lack transparency. Similarly, hybrid ML–DL frameworks [7,11] were optimized for IoT environments rather than cloud infrastructures. The Snort-OSSEC hybrid IDS offers balanced accuracy and efficiency through a practical, open-source alternative accessible to enterprises with limited computational resources.

The Snort–OSSEC hybrid model also presents certain limitations. The system was evaluated within a small-scale cloud testbed and restricted to four attack types, excluding more sophisticated adversarial techniques such as ransomware and advanced persistent threats (APTs). Moreover, while the hybrid IDS demonstrated high accuracy, it lacks adaptive learning capabilities for detecting zero-day threats and operates strictly as an IDS rather than an IPS. The limitations that come with the hybrid model are a prerequisite for future research as outlined in Section 6, which includes scaling the framework to multi-tenant clouds, widening the attack coverage, inclusion of adaptive learning, and evolving toward automated prevention mechanisms.

5.2. Open Challenges and Future Work

Although the proposed hybrid IDS demonstrated strong results in a controlled testbed, several limitations highlight opportunities for future research. First, the evaluation was restricted to a small-scale virtualized cloud environment. Future research should explore the validation of the framework on a large-scale, multi-tenant infrastructure to examine the scalability and performance of the model when used in a diverse workload. Furthermore, simulation was carried out on four categories of attacks: port scanning, denial-of-service (DoS), brute-force login, and user-to-root (U2R). Expanding the model's attack set to include ransomware, insider threats, and advanced persistent threats (APTs) would enable a critical evaluation of system effectiveness.

The study also lacks adaptive learning mechanisms. Although the hybrid model effectively reduced false alarms, its capacity in detecting zero-day attacks remains limited. The inclusion of online learning, federated learning, or reinforcement learning can further enhance the model's adaptability against evolving threats. Finally, the system functionality is currently just an intrusion detection system. Transitioning the system into an intrusion prevention system (IPS) by automating responses such as virtual machine isolation or IP blocking would substantially enhance its practical utility, but it also introduces potential concerns regarding service continuity. Addressing these open challenges will be critical to advancing hybrid IDS solutions into enterprise-ready, next-generation cloud security frameworks.

5.3. Contribution of the Study

This study contributes to cloud security research by proposing and validating a hybrid intrusion detection system (IDS) that integrates Snort (N-IDS) and OSSEC (H-IDS) for cross-layer alert correlation. Unlike previous works that relied solely on either standalone signature-based systems or computationally intensive deep learning frameworks, the proposed model demonstrates cost-effectiveness, interpretability, and scalability. It provides a transparent detection process, reduces false alarms through dual validation, and offers a strong foundation for forensic analysis by combining network- and host-level mechanisms. The research further contributes by offering an open-source, real-world testbed implementation, thus bridging the gap between theoretical models and practical deployment in enterprise cloud infrastructures.

5.4. Key Findings

The results confirm three major findings:

1. Superior Performance of Hybrid IDS: The hybrid framework achieved 97.1% accuracy, 94.1% detection rate, and a remarkably low 0.2% false alarm rate, outperforming both Snort-only and OSSEC-only deployments.

2. Validated Case-Based Detection: Attack simulations showed that hybrid correlation not only improved detection but also reduced false positives and enriched forensic trails, particularly in cases such as port scanning, brute-force login, and user-to-root exploits.
3. Balanced Contribution to State of the Art: Compared with previous IDS research, the hybrid IDS delivered competitive accuracy while maintaining efficiency and interpretability, offering a practical middle ground between lightweight standalone systems and complex deep learning frameworks.

6. Conclusions

This study demonstrates that a hybrid IDS architecture integrating Snort and OSSEC can offer a robust, efficient, and interpretable solution for enhancing cloud security. With the incorporation of cross-layer correlation, the model addresses the limitations that are common with standalone systems by delivering an improved detection accuracy, reduction of false positives, and enhanced forensic analysis. Comparative benchmarking confirms that the proposed system performs on par with or surpasses state-of-the-art IDS approaches, while remaining more cost-effective and readily deployable in real-world environments.

However, the limitation of the study is that it was carried out using a small-scale testbed deployment, the range of attack types is just four, and it also lacks adaptive learning and the ability to prevent attacks. These limitations open clear directions for future work, including scaling multi-tenant clouds, expanding attack coverage to advanced persistent threats, integrating adaptive learning for zero-day detection, and evolving into an intrusion prevention system (IPS). Finally, this research advances the cloud computing and cybersecurity landscape with a practical and transparent hybrid IDS framework that strengthens trust and reliability in cloud security monitoring.

List of Abbreviations

IDS	Intrusion Detection System
HIDS	Host-based Intrusion Detection System
NIDS	Network-based Intrusion Detection System
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
VM	Virtual Machine
U2R	User-to-Root Attack
DoS	Denial of Service
DDoS	Distributed Denial of Service
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
FTP	File Transfer Protocol
IPS	Intrusion Prevention System
TP	True Positive
TN	True Negative
FP	False Positive
FN	False Negative
ACC	Accuracy
DR	Detection Rate
FAR	False Alarm Rate
MCC	Matthews Correlation Coefficient
ROC	Receiver Operating Characteristic
PRC	Precision-Recall Curve

Author Contributions

I.O.I.: contributed to the study by working on the systematic review using all the aforementioned platforms, data analysis, corrections of texts, the formulation of the framework and the algorithm, design of graphics, and flowcharts. A.U.T.: supervised the research. All authors have read and agreed to the published version of the manuscript.

Availability of Data and Materials

The dataset generated from the testbed setup and used to evaluate the study can be provided on request.

Consent for Publication

No consent for publication is required, as the manuscript does not involve any individual personal data, images, videos, or other materials that would necessitate consent.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

The study did not receive any external funding and was conducted using only institutional resources.

Acknowledgments

We would like to acknowledge that Grammarly and Copyleak AI platforms were used to improve the grammatical structure of the study.

References

[1] M. Sajid, K. R. Malik, A. Almogren, T. S. Malik, A. H. Khan, J. Tanveer, and M. U. Rehman, "Enhancing Intrusion Detection: A Hybrid Machine and Deep Learning Approach," *Journal of Cloud Computing*, vol. 13, 123, 2024. [CrossRef]

[2] S. M. Othman, A. Y. Al-Mutawkkil, and A. M. Alnashi, "Survey of Intrusion Detection Techniques in Cloud Computing," *Sana'a University Journal of Applied Sciences and Technology*, vol. 2, no. 4, pp. 363–374, 2024. [CrossRef]

[3] L. Boukela, G. Zhang, M. Yacoub, and S. Bouzefrane, "A Near-Autonomous and Incremental Intrusion Detection System Through Active Learning of Known and Unknown Attacks," in *2021 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)*, Chengdu, China, 2021, pp. 374–379. [CrossRef]

[4] V. Govindarajan and J. H. Muzamal, "Advanced Cloud Intrusion Detection Framework Using Graph-Based Features, Transformers, and Contrastive Learning," *Scientific Reports*, vol. 15, no. 1, 20511, 2025. [CrossRef]

[5] U. Kumar and B. N. Gohil, "A Survey on Intrusion Detection Systems for Cloud Computing Environment," *International Journal of Computer Applications*, vol. 109, no. 1, pp. 6–15, 2015. [CrossRef]

[6] A. Giessmann and K. Stanoevska-Slabeva, "Business Models of Platform as a Service (PaaS) Providers: Current State and Future Directions," *Journal of Information Technology Theory and Application (JITTA)*, vol. 13, no. 4, pp. 31–55, 2013. [View Online]

[7] T. Gu, B. Dolan-Gavitt, and S. Garg, "BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain," *IEEE Access*, vol. 7, pp. 47230–47244, 2019. [CrossRef]

[8] C. Mazzariello, R. Bifulco, and R. Canonico, "Integrating a Network IDS into an Open-Source Cloud Computing Environment," in *6th International Conference on Information Assurance and Security*, Atlanta, GA, USA, 2010, pp. 265–270. [CrossRef]

[9] Gupta, M., "Hybrid Intrusion Detection System: Technology and Development," *International Journal of Computer Applications*, vol. 115, no. 9, pp. 5–8, 2015. [CrossRef]

[10] E. U. H. Qazi, M. H. Faheem, and T. Zia, "HDL-NIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System," *Applied Sciences*, vol. 13, no. 8, 4921, 2023. [CrossRef]

[11] M. Kimanzi, J. Odhiambo, and J. Mwangi, "Deep Learning Algorithms in Intrusion Detection Systems: A Comprehensive Review," *arXiv preprint*, 2024. [CrossRef]

[12] N. Wali Khan, M. S. Alshehri, M. A. Khan, S. Almakdi, N. Moradpoor, A. Alazeb, S. Ullah, N. Naz, and J. Ahmad, "A Hybrid deep learning-based intrusion detection system for IoT networks," *Mathematical Biosciences and Engineering*, vol. 20, no. 5, pp. 8493–8510, 2023. [CrossRef]

[13] N. Pandeeswari and G. Kumar, "Anomaly Detection System in Cloud Environment Using Fuzzy Clustering-Based ANN," *Mobile Networks and Applications*, vol. 21, no. 3, pp. 494–505, 2026. [CrossRef]

[14] O. Belarbi, M. Guerroumi, and A. Serhrouchni, "Federated Deep Learning Intrusion Detection System for IoT Networks," arXiv preprint, 2023. [CrossRef]