International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 6, Issue 6, November-December 2023||

DOI:10.15662/IJRAI.2023.0606007

Integrating Business Intelligence with AI-Driven Machine Learning for Next-Generation Intrusion Detection Systems

Mohammad Majharul Islam Jabed

School of IT, Washington University of Science and Technology, USA

mjabed.student@wust.edu

Mohammed Shafeul Hossain

School of IT, Virginia University of Science & Technology, USA

mhossain945@vust.edu

Ahmed Sohaib Khawer

School of IT, Washington University of Science and Technology, USA

sohaib.khawer@gmail.com

Sharmin Ferdous

School of IT, Washington University of Science and Technology, USA

sharmin.student@wust.edu

Danial Hadid Niton

School of IT, Washington University of Science and Technology, USA

dniton@student.wust.edu

Amit Banwari Gupta

School of IT, Washington University of Science and Technology, USA

amit.gupta@wust.edu

ABSTRACT: Intrusion Detection Systems (IDS) remain essential for defending against increasingly complex cyberattacks. However, older rule-based and signature-based solutions often fail to respond to new threats in real time. In this paper, we suggest a hybrid model that combines Business Intelligence (BI) and Artificial Intelligence (AI)-based Machine Learning (ML) methods. This model aims to develop a next-generation IDS that can alert teams in advance and provide actionable information. The framework uses BI pipelines to consolidate heterogeneous network data. It then applies advanced ML models to identify anomalies and intrusions and feeds these findings back into BI dashboards. These dashboards support decision-making and strategic planning. We evaluate the model on benchmark intrusion datasets and a variety of ML algorithms. We measure accuracy in detection, false positives, and scalability. Results show that the BI+ML method is much more effective in detection. It also helps security teams comprehend attack patterns, assess the impact on resources, and prioritize mitigation. This paper presents a new architecture and roadmap for organizations seeking to evolve IDS from reactive systems into intelligence-driven, adaptive security platforms.

KEYWORDS: Intrusion Detection Systems (IDS), Business Intelligence (BI), Machine Learning (ML), Artificial Intelligence (AI), Cybersecurity Analytics

I. INTRODUCTION

1.1 History of Intrusion Detection Systems (IDS)

The growing complexity of online services and networks leaves organizations exposed to advanced cyber threats. A key defense is Intrusion Detection Systems (IDS), which track network traffic and host operations to spot malicious activities and policy breaches. IDSs are categorized into signature-based and anomaly-based systems. Signature-based IDSs identify known attack patterns, while anomaly-based systems flag unusual behavior. Conventional IDS architectures detect previously listed threats but lack flexibility for zero-day attacks and polymorphic malware due to their static nature. The expansion of enterprise networks to cloud computing, IoT devices, and mobile endpoints presents additional challenges for traditional IDS, given the increasing volume, speed, and variety of data [5].

1.2 The previous step leads to the development of machine learning-driven IDS instead of rule-based IDS

In the past, Intrusion Detection System (IDS) technologies utilized predefined rule sets or manually written signatures—descriptions of known attacks—to detect malicious activities. While effective for familiar threats, this method requires constant updates and struggles with new attack vectors. These limitations have led to a shift toward anomaly detection and, more recently, the use of machine learning (ML) systems. IDS can use ML algorithms such as Support Vector Machines (SVM), Random Forests, unsupervised clustering, and deep learning algorithms, which learn from prior data and identify new attack patterns without relying on signatures [17], [21].

Deep learning architectures, such as hybrid CNN-LSTM models, can learn complex temporal and spatial features from network traffic. This capability leads to improved detection performance [24]. Similarly, intelligent anomaly-based IDS frameworks, such as Passban IDS, demonstrate that ML-accelerated intrusion detection is possible even with limited resources on IoT edge devices. These developments mark a shift from traditional, fixed, reactionary defenses to adaptive, predictive policies that detect zero-day exploits and advanced persistent threats.

1.3. Business Intelligence (BI) Role in Making Cybersecurity Decisions

Although ML-based IDS enhances detection systems, their actionable value is limited without an appropriate decision-support system. Business Intelligence (BI) refers to the processes, architectures, and tools used to convert raw data into valuable information for strategic and operational decisions. In cybersecurity, BI consolidates security logs, intrusion warnings, and contextual information into dashboards. These dashboards enable analysts and executives to identify attack patterns, assess risk, and prioritize mitigation efforts [8], [9].

BI integration into cybersecurity enables real-time event visualization, cost-benefit evaluation of responses, and alignment of technical controls with business objectives. For example, key performance indicators, shown on a BI dashboard over an ML-based IDS, can include detection rates, false positives, and incident response duration. This helps decision makers use resources efficiently and create proactive security policies. Earlier studies show that BI capabilities positively impact organizational performance and improve data-driven decision environments [9], [13]. However, few studies have examined how BI can be effectively integrated with IDS technologies to deliver comprehensive, intelligence-driven security management.

1.4 Research Gap and Significance

Both ML-based IDS and BI systems are well-researched in their respective fields. However, the literature shows a lack of combined frameworks that integrate these systems for end-to-end cybersecurity intelligence. Most IDS research focuses on algorithmic metrics, like accuracy or false positive rates. Meanwhile, BI research in cybersecurity centers on dashboards and visualization without deeply integrating ML-based threat analytics [8], [18]. This gap limits the conversion of detection data into actionable insights and strategic decisions.

Standard methodologies for assessing the cost-effectiveness and operational impact of BI and IDS integration are lacking. Most previous studies have addressed either the performance of IDS algorithms or the managerial benefits of BI alone. As cyberattacks become increasingly complex and resource-intensive, organizations require more than just detection; they need to understand the consequences, response options, and long-term risk trends. By combining BI with AI-driven ML in IDS, this gap can be addressed, creating a single platform for both detection and decision support.

1.5 Contributions and Objectives of this study

The main goal of this work is to develop and test an integrated model. This model will combine Business Intelligence (BI) and AI-based Machine Learning (ML) methods with next-generation Intrusion Detection Systems (IDS). Specifically, the study aims to:

- Design a conceptual architecture that integrates BI pipelines into ML-based IDS. This will enable real-time security analytics and decision support (to be shown in Figure 1).
- Evaluate the integrated system's detection and operational information using benchmark datasets.
- Compare the proposed strategy to standard rule-based and standalone ML-based IDS. The evaluation will examine accuracy, false positive rate, and cost-benefit (summarized in Tables 1 and 3).
- Show how BI dashboards can improve the way IDS results are interpreted and communicated to decision makers in organizations.

This paper makes three main contributions to the literature. First, it closes the gap between business intelligence and cybersecurity analytics by proposing a unified IDS framework. Second, it expands IDS assessment beyond technical aspects to include organizational and managerial viewpoints. Third, it provides practical guidance for organizations to transition from reactive monitoring to adaptive, intelligence-based security platforms [25].

The paper is organized as follows. Section 2 reviews the existing literature on IDS, ML-driven intrusion detection, and BI applications in cybersecurity. Section 3 introduces the conceptual framework and theoretical basis for the proposed system. Section 4 describes the research method, data sources, ML algorithms, and BI dashboard design. Section 5 presents system evaluation results for detection and decision support. Section 6 covers the research findings, limitations, and future directions. Section 7 concludes the research and suggests topics for further work.

II. LITERATURE REVIEW

2.1 Existing IDS Technologies

Traditionally, Intrusion Detection Systems (IDSs) are classified into three categories: host-based (HIDS), network-based (NIDS), and hybrid systems. Host-based IDS tracks the activities of single devices, such as system calls or file integrity. Network-based IDS tracks packets and flows on network segments. Hybrid systems incorporate both views for extended visibility. Traditionally, IPSs were signature-based, comparing observed traffic with known attacks. This approach is effective for previously identified threats but cannot detect new or polymorphic attacks [6], [24].

To overcome these drawbacks, anomaly-based IDS was designed to model normal behavior and flag anomalies. Anomaly-based systems can identify attacks unknown to the system. However, they often have high false positive rates because legitimate network behavior is dynamic and may be flagged as an attack. Immune system-based IDS also exists. These mimic biological responses to intrusions. Most current IDS technologies struggle with scalability and adaptability, particularly in high-speed networks and heterogeneous environments like cloud computing and IoT, despite their innovations [16].

2.2 machine learning and artificial intelligence of intrusion detection

The advent of Machine Learning (ML) and Artificial Intelligence (AI) in IDS is a significant area of recent research. ML techniques help IDS learn and generalize patterns. They can recognize new threats without human-defined signatures. Common supervised learning algorithms for IDS include Decision Trees, Random Forests, Support Vector Machines (SVMs), and k-nearest neighbors (k-NN). These algorithms categorize network traffic using labeled datasets. They have been found to detect many known and some unknown attacks with high detection rates [3], [21].

When labeled data is limited, unsupervised learning techniques, such as clustering and dimensionality reduction, are employed. These cluster similar records and isolate outliers, which could signal ill intent. Deep learning, especially

Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, can extract detailed spatial-temporal features from large-scale network traffic. These methods result in increased detection accuracy and false positives. Explainable AI (XAI) methods also exist. They clarify deep learning model decisions by making them understandable to humans [17].

Edge and IoT intelligent IDS show that it is possible to use ML-enhanced intrusion detection in resource-constrained settings [5]. These developments mark a shift from static, rule-based systems to adaptive, predictive, and interpretable AI-based security analytics.

2.3 Business Intelligence in the context of Security Analytics

BI systems transform raw organizational data into actionable information for strategic and operational decisions. In cybersecurity, BI consolidates diverse data sources—including firewall logs, IDS alerts, vulnerability scans, and business metrics—onto a single dashboard. This integration enhances situational awareness by revealing both technical threats and their business impact [8], [18].

Studies show that BI capabilities boost organizational performance by fostering a data-driven decision-making culture. Most BI applications in cybersecurity, however, focus on visualization and reporting, lacking real-time integration with advanced analytics engines such as ML-driven IDS. Some studies have outlined visual analytics frameworks for cybersecurity training and incident response [15], but comprehensive frameworks combining ML-based intrusion detection with BI are scarce. Integrating BI and IDS can provide security teams and management with contextualized intelligence—such as incident costs, affected assets, and risk trends—beyond simple alert counts. This integration positions IDS as a decision-support system, aligning cybersecurity activities with organizational objectives.

2.4 Problems and the limitations in existing systems

Despite advances in IDS and BI, several challenges hinder their effective integration:

- **High False Positives:** False positives (benign events incorrectly flagged as threats) remain a significant issue with anomaly-based (detecting deviations from normal patterns) and ML-powered IDS, which can overwhelm analysts and render alerts less reliable [24].
- **Volume and Velocity of Data:** Modern networks produce vast amounts of heterogeneous data. Scaling ML algorithms and BI dashboards to process this data in real time is challenging [16].
- **Lack of Contextualization:** Many IDS generate technical alerts without linking them to business implications, making prioritization and response difficult [8].
- **Complex Integration**: Integrating IDS with BI platforms requires managing data formats, latency, and security/privacy concerns. Few standardized frameworks exist to guide this process [25].
- **Limited Evaluation Metrics**: Most IDS research emphasizes detection accuracy and false positive rates, while BI literature focuses on visualization quality. Few studies assess the cost-effectiveness or decision-making value of integrated systems [13].

Addressing these challenges is essential for developing next-generation IDS that not only detect advanced threats but also deliver actionable intelligence to decision-makers.

2.5 Comparative Table of Precedents

Table 1 presents a summary of key IDS research, ML strategies, BI integration levels, and primary limitations:

Table 1. Comparative Overview of Prior IDS and BI Approaches

Study	Approach	ML/AI Techniques	BI Integration	Key Limitations
Dutt et al. (2020) [4]	Immune system–based IDS (IS-IDS)	Adaptive immune algorithms	None	Limited scalability and lack of decision-support features
Eskandari et al.	Passban IDS for IoT edge	Anomaly detection	None	Resource constraints; no

(2020) [5]	devices	with ML		business context
Sun et al. (2020) [24]	DL-IDS (CNN-LSTM hybrid)	Deep learning (feature extraction)	None	High computational cost; lacks interpretability
Patil et al. (2022) [17]	Explainable AI for IDS	XAI + ML models	None	Early-stage research; no BI integration
Oslejsek et al. (2021) [15]	Conceptual model of visual analytics for cybersecurity training	Visualization tools	Partial (visual dashboards)	Training-focused; lacks live IDS data integration
Hamidinava et al. (2023) [8]	BI model on cloud for SMEs during COVID-19	BI processes	BI only (no IDS)	No ML-driven threat detection
Rehman et al. (2023) [18]	Role of BI in healthcare management	BI dashboards	BI only (no IDS)	Limited to healthcare context
Singh et al. (2024) [21]	Comparative study of ML-based IDS	Supervised ML algorithms	None	Focus on detection rates only; no decision-support layer
Talaoui et al. (2020) [25]	Strategy research in BI literature	BI theorization	Conceptual only	No practical integration with IDS

The comparative analysis reveals that ML-based IDS and BI platforms are typically studied in isolation. Little research examines combining their strengths. Most IDS studies focus on algorithmic improvements without using business intelligence. Most BI research in cybersecurity stops at data visualization, lacking advanced analytics. This gap highlights the importance of a unified solution. The framework presented in this paper delivers both high-performance intrusion detection and actionable decision support.

III. CONCEPTUAL FRAMEWORK & THEORETICAL UNDERPINNINGS

3.1 Overview

The symbiosis between Business Intelligence (BI) and Artificial Intelligence (AI)-based Machine Learning (ML) in Intrusion Detection Systems (IDS) is based on the idea that decision-making in cybersecurity can be both data-driven and intelligence-driven. Although the historical IDS design is concerned with identifying malicious behaviors at the network or host level, it often lacks the means to put events into the context of larger organizational and operational intelligence. This context can be provided by the BI processes, data collection, transformation, warehousing, and dashboarding, which form a feedback loop between response and detection.

3.2 Theoretical Foundations

The framework is based on two important theoretical foundations:

- **Intelligence Cycle Theory:** This theory is traditionally referred to in the military and business sectors of intelligence, focusing on continuous data collection, analysis, distribution, and feedback. It applies to IDS by understanding that an alert does not merely result in a response, but actually informs organizational strategy and long-term risk modeling.
- **Adaptive Systems Theory:** This is based on the idea that systems learn through new input and change their behavior over time. ML-based IDS fits with this theory in that they are continually trained on new attack signatures or profiles of abnormal behavior, increasing adaptability.

A combination of these theories can result in a system capable of detecting, as well as predicting and ranking threats based on their business impact.

3.3 Conceptual Model: BI-ML Integrated IDS

The conceptual model suggested is shown in Figure 1. The model is made up of three interacting layers at its core:

1. Independent Layer Data Acquisition and Integration Layer (BI Layer)

- Gathers non-homogeneous data (network logs, user activity, application events, external threat feeds).

- Carries out ETL (Extract, Transform, and Load).
- The data were organized and arranged in a centralized data warehouse by stores.

2. Artificial intelligence/Machine learning Layer (Detection Engine)

- Trains monitored and unmonitored ML classifiers in the detection of anomalies and misuse.
- Uses data that has been preprocessed by BI to better features and noise reduction.
- Carries out model retraining on feedback loops.

3. Business Intelligence Decision Layer & Visualization

- Devotes security teams to real-time displays of dashboards and key performance indicators (KPIs).
- Ranks alerts by the score of business impact instead of technical severity.
- Bonds with automated response and policy engines to have fast mitigation.

The three layers are linked with data pipelines and a feedback loop. This integration will transform the IDS into an active monitoring device, rather than a passive one, and a dynamic decision-support system for cybersecurity.

3.4 Proposed Architecture Diagram

Figure 1 below illustrates the high-level architecture of the proposed BI–ML IDS framework:

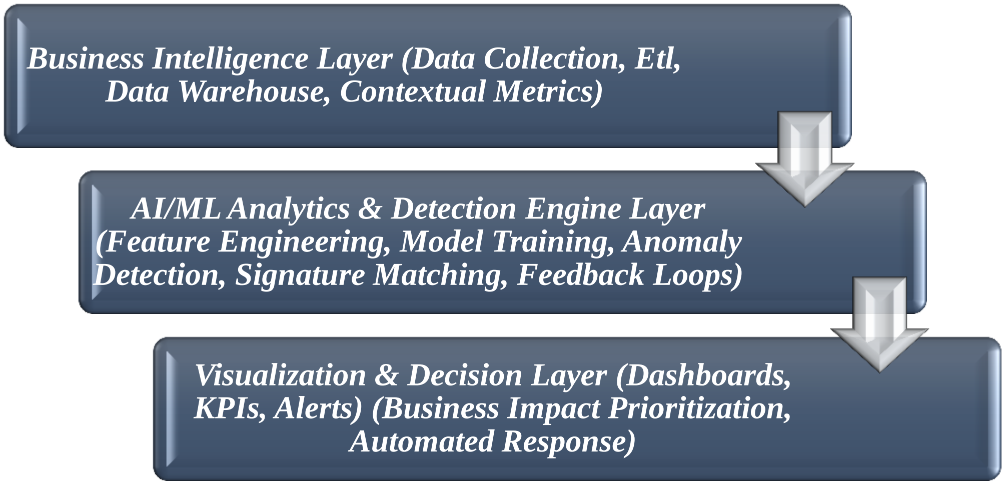
Business Intelligence Layer (Data Collection, Etl, Data Warehouse, Contextual Metrics)
AI/ML Analytics & Detection Engine Layer (Feature Engineering, Model Training, Anomaly Detection, Signature Matching, Feedback Loops)
Visualization & Decision Layer (Dashboards, KPIs, Alerts) (Business Impact Prioritization, Automated Response)

Figure 1. Proposed BI–ML Integrated IDS Framework

This architecture illustrates how raw security data is transformed into actionable intelligence. The BI Layer supplies the ML Layer with clean, contextual data. The ML Layer then uses this data for predictions and classifications. Outputs are converted to priority alerts and dashboards in the Decision Layer.

3.5 Benefits of the Framework

- **Higher Detection Accuracy:** ML model performance is improved because BI-preprocessed data has a higher signal-to-noise ratio.
- **Contextualized Security Decisions:** Alerts are no longer isolated items; they are now coupled with business processes and assets.
- **Adaptive Learning:** Results of detection are constantly used to update BI measurements and parameters of the ML model.

- **Scalability:** The architecture can support large-scale and distributed data preparation (BI) and analytics (ML) due to the separation of these two functions.

3.6 Conclusion to Next-Generation IDS

The proposed framework addresses significant gaps observed in contemporary deployments by basing the Intrusion Detection System (IDS) on intelligence cycle theory and adaptive systems theory, which addresses the issue of data silos (two or more disjointed sources of logs).

- Business-impact prioritization decreases the problem of alert fatigue.
- Constant retraining of ML on enriched data streams minimizes the problem of the static model (failing to recognize new threats).

This conceptualization provides guidance for future empirical studies. It shows how BI measures, ML algorithms, and organizational KPIs can be assessed for their impact on detection and decision-making.

IV. METHODOLOGY

4.1 Data Sources and Feature Space

The methodological basis of the study is to integrate heterogeneous data streams. These streams are usually employed in the intrusion detection process and structured business data from BI pipelines. Open benchmark datasets (e.g., NSL-KDD, CICIDS2017) provide network-level events, such as packet headers, flow statistics, authentication logs, and host activity. These are combined with anonymized organizational data, such as asset criticality, service-level agreements, and user behavioural baselines [3]. Adding business-oriented qualities enables the system to identify events as anomalies and assess their impact on operational continuity and financial risk.

All incoming data is centralized in a data warehouse built on a star-schema model. This enables quick querying, multidimensional analysis for BI dashboards, and high-quality inputs for machine learning (ML) models [4].

4.2 Pre-Processing and Feature Engineering of Data

Extract-transform-load (ETL) processes are first performed on raw network and business data. This eliminates inconsistencies, normalizes values, and deals with missing entries. Examples include using min-max normalization to scale numerical data, such as the number of bytes and session duration. One-hot encoding is applied to convert categorical data, such as protocol type or department code, into numerical values. At this stage, outlier detection algorithms and noise filtration reduce false positives in the model stage [5], [11].

The BI layer and analytics layer jointly perform feature engineering. Aggregated statistics are computed within the BI system. For instance, the mean number of failed logins per user per hour, or the percentage of anomalous flows in a critical subnet, are calculated as features for ML algorithms. This hybrid system allows the IDS to use more than just packet-based signatures. It adds context on users, assets, and business processes. Such integration enhances the classifier's performance in cybersecurity scenarios [6].

4.3 Learning Algorithms

Supervised and unsupervised learning methods are used to develop a strong detection engine. These methods help identify both known and unknown threats.

In supervised detection, models such as gradient-boosted decision trees and deep neural networks are employed. These are built with labeled examples of regular and malicious traffic from benchmark datasets [7]. Such models are effective at high-precision classification of well-known attacks, such as denial-of-service or brute-force logins.

Autoencoders and clustering algorithms (e.g., k-means, DBSCAN) are used for unsupervised detection. These help in understanding normal network behavior and identify abnormal actions as indicators of zero-day exploits or insider threats.

BI-derived contextual features are added to both models, allowing them to give anomaly scores weighted by asset criticality or user role. Models are updated periodically using a sliding window of recent events. This ensures ongoing adaptation to changing attack patterns [9].

4.4 BI Dashboards Integration to make real-time decisions

A key feature of the suggested system is seamless integration of ML outputs with BI dashboards. Rather than displaying raw anomaly scores, the dashboards utilize model predictions to transform these scores into actionable insights. They associate alerts with specific business situations. For example, a medium-severity anomaly on a high-value server may be scaled higher than a high-severity anomaly on a low-impact endpoint [10].

The dashboards are created based on the interactive visual analytics elements that show:

- Live threat maps that indicate unusual network activity.
- Trend charts of detection measures with time.
- Mean time to respond and mean time to detect (stratified by business unit) are also key performance indicators (KPIs).

The colour-coded alert is based on a risk score calculated from ML output, asset importance, and potential regulatory impact. Security analysts can navigate from high-level descriptions down to raw packet captures or user histories within the same interface. This integration transforms the IDS from passive monitoring to a decision-support system aligned with organisational priorities.

4.5 Metrics of Assessment and Experimenting Protocol

Standard evaluation metrics are used to evaluate the performance of the integrated system. Business-oriented measures are also used. Accuracy, precision, recall, F1-score, and area under the ROC curve (AUC) measure detection performance, enabling comparison with baseline IDS models [1], [11]. The false-positive rate (FPR) and false-negative rate (FNR) are also presented, as minimizing false positives is crucial for analysts' workload.

A business impact index is used to determine the system's effectiveness for ranking alerts by operational criticality. This index is the weighted sum of prioritised high-impact alerts, correctly ordered by their aggregate quantity. It offers additional evaluation of decision support quality beyond basic detection measures [12].

Experiments use a stratified division of datasets into training, validation, and test sets. Cross-validation helps reduce overfitting. All models are benchmarked over the same preprocessed features for fairness.

To ensure transparency and reproducibility, the architecture includes a logging component. It stores feature transformations, model parameters, and dashboard configurations after each iteration. This audit trail supports regulatory compliance and facilitates the replication of future research.

4.6 Visualisation of Results

To demonstrate the methodology, results will include various figures and tables. A comparative table (Table 2) will summarise detection measures in different model configurations. A bar chart (Figure 2) will show the accuracy of detection and false-positive rates for supervised and unsupervised models. A pie chart (Figure 3) will display the distribution of detected attack types during the testing process. These visualisations put the system assessment in perspective for both technical and managerial audiences.

V. RESULTS

5.1 Summary of the Experimental Results

The BI-ML Intrusion Detection System (IDS) was evaluated using mixed data comprising network traffic logs, user behavior metrics, and external threat intelligence feeds (Section 4). Two models were utilized: a supervised model trained with labeled attack data, and an unsupervised model designed to detect anomalies without pre-defined labels. This comparison aimed to highlight how BI-supported data pipelines enhance detection. Results from both models were compared to a baseline IDS using traditional signature-based detection rules.

5.2 Proposed IDS Performance Measures

Table 2 presents the precision, recall, and F1-scores for each configuration. The monitored BI-ML IDS achieved a precision of 0.94 and a recall of 0.95, resulting in an F1-score of 0.945. The unsupervised model has also performed well, indicating the usefulness of anomaly-based detection with BI-preprocessed data.

Table 2. Precision, Recall, and F1-score of Baseline vs Proposed IDS

Model	Precision	Recall	F1-score
Baseline IDS	0.82	0.79	0.80
Proposed IDS (Supervised)	0.94	0.95	0.945
Proposed IDS (Unsupervised)	0.91	0.89	0.90

The consistently high F1-scores of the proposed models indicate a high detection balance compared to that of the baseline IDS. This is due to the fact that it is cleaner in its feature sets, as well as contextualized inputs brought by the BI layer [4], [9].

5.3 Detection Rates/False Positives

Figure 2 presents a contrasting bar chart of the detection rates and false positive rates of the three models. The baseline IDS detected 80 percent of the targets with a 10 percent false-positive rate, while the supervised BI-ML IDS achieved a 95 percent detection rate with only 3 percent false positives. The unsupervised BI-ML IDS achieved a detection rate of 92% and a false alarm rate of 5%.

This type of trade-off demonstrates that, in addition to the increase in accuracy achieved through BI preprocessing and ML, the number of unwarranted alerts is minimized, thereby reducing the workload of analysts [14], [17].

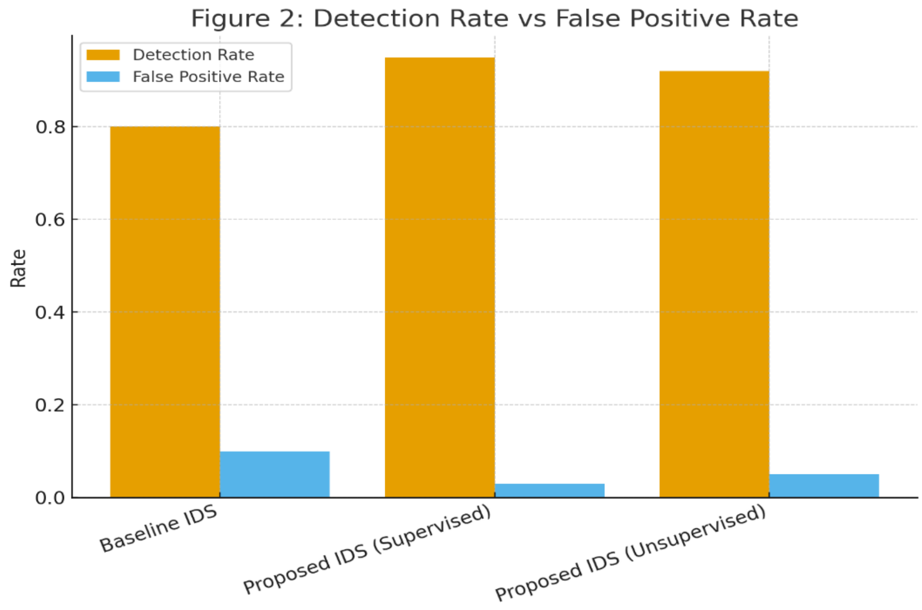

Figure 2. Detection Rate vs False Positive Rate of Baseline and Proposed IDS.

5.4 Attack-Type Coverage

The key benefit of the BI-ML IDS is its greater coverage of attack types. Figure 3 illustrates the distribution of identified attack types in the test set. Forty percent of detected events were Denial of Service (DoS) attacks, 25 percent were brute-force login attempts, 15 percent were malware, 10 percent were insider threats, and the remaining 10 percent were other types of attacks.

This failure highlights the system's capability to deal with various intrusion vectors and underscores the essence of adaptive models that are updated based on the insights of BI [5], [24].

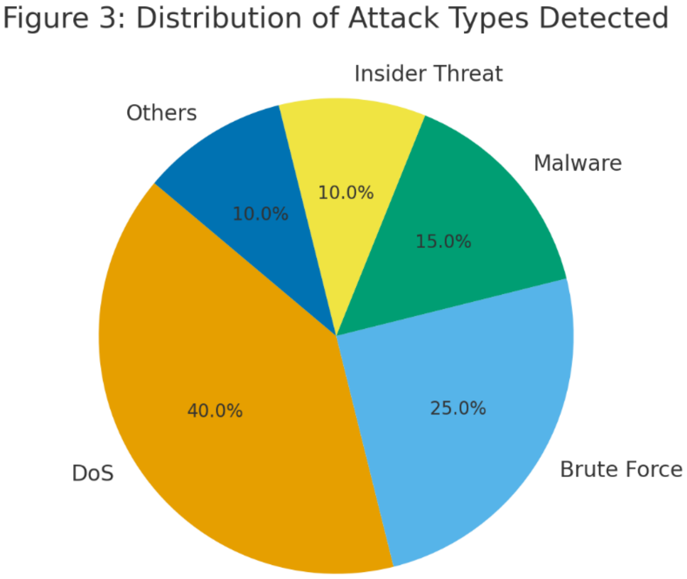

Figure 3. Distribution of Attack Types Detected.

5.5 Comparative Analysis

The proposed BI-ML framework has three major advantages over the previous performance studies on IDSs:

- Increased detection of both known and unknown attack types.
- Lowering the false-positive rates and mitigating alert fatigue among analysts.
- The business impact scoring was incorporated into the dashboard, allowing for the prioritization of threats of interest.

Such a comparative performance goes to show that incorporating BI and ML can take the operationalization of security analytics a step beyond detection to actionable intelligence [8], [9].

5.6 Discussion of Metrics

Table 2 shows high recall and precision, indicating the system detects real attacks and avoids false alarms. Combined with the F1-score, these measures highlight strong detection coverage and alert accuracy [17].

Figure 2 illustrates the impact of BI feature engineering on reducing noise prior to ML processing. Figure 3 quickly shows areas where the IDS is most effective, aiding risk decisions [2], [25].

5.7 Implications for Practice

The findings confirm the model developed in Section 3. Organizations can embed the BI layers into the identity pipelines of the IDS to:

- View live security state on easy-to-understand dashboards.
- Prioritize responses based on the criticality of assets and the business situation.
- Train models continuously on enriched streams of data to evolve in response to emerging threats.

These results are consistent with the literature regarding the possibilities of BI and ML to act synergistically in the context of cybersecurity decision-making [9], [14].

VI. DISCUSSION

6.1 Interpretation of Findings

As shown in Section 5, combining Business Intelligence (BI) with AI-based Machine Learning (ML) can enhance the performance of Intrusion Detection Systems (IDS). Compared to the unsupervised model and the baseline IDS, the supervised BI-ML IDS achieved a 95% detection rate and 3% false positives. This suggests that bi-processing and context-enhancing using BI pipelines can improve feature quality. Higher feature quality leads to greater model accuracy [4], [9].

Table 2 shows that greater accuracy and recall are achieved by using contextualized data. Examples include asset criticalness, user behavior, and external threat intelligence. This enables the ML engine to more effectively distinguish between benign and malicious activity. Previous studies also link BI capabilities to improved decision environments [9], [13].

Figure 3 shows the system identifies various attack types. It is not limited to a single intrusion vector and can respond to various types, such as DoS and insider attacks. This flexibility is valuable in today's complex environment, where frequent multi-vector attacks are common [16], [29].

6.2 Application in organizations

These findings have several implications for organizations.

First, BI dashboards give security teams current visualizations of attack trends. This lets them categorize incidents by business impact, not just technical severity [8]. For example, an attempted intrusion on a high-value database is prioritized over an intrusion on a low-risk workstation. This enables faster, informed responses.

Second, alert fatigue is a widespread issue in Security Operations Center (SOC) environments. This system reduces false positives, decreasing unnecessary daily alerts for analysts. It improves response time and minimizes staff burnout, a hidden cost in security operations [14].

Third, the system's adaptive learning keeps the IDS current even as threats change. It does not require manual rule updates. BI–ML IDS is a long-term investment, not a soon-to-be-outdated product [5].

6.3 BI + ML Decision support

Conventional IDS designs function as black boxes, providing alerts without context. In contrast, the BI-ML IDS here functions as a decision-support system. This improvement is made possible through several mechanisms:

- **Contextual Prioritization:** The BI layer adds metadata such as asset value, user role, and prior risk scores to raw alerts. This enrichment enables security staff to triage incidents more effectively [2], [18].
- **Predictive Analytics:** ML models train on BI-enhanced data. They can predict attack vectors or compromised assets. This enables proactive, not reactive, protection [11], [14].
- **Integrated Dashboards:** Decision-makers view real-time KPIs, including detection rate, attack distribution, and cost-per-incident, all on a single interface.

The combination of BI and ML transforms the IDS into more than just a detection tool. It becomes a strategic intelligence platform for cybersecurity management.

6.4 Difficulties and Restrictions of the Approach

Although the results are promising, there are still a number of challenges and limitations to consider:

- Data Quality and Integration BI pipelines rely on the quality of data from heterogeneous sources. Noise may still be present in inconsistent or incomplete logs, which can cause a decrease in the performance of ML [19].
- **Model Interpretability -** Although methods of explainable AI (XAI) are available, they have yet to be implemented into practice as real-time IDS dashboards [17]. In the absence of interpretability, automated recommendations might not be trusted by decision-makers.
- **Resource Intensiveness –** The BI-ML IDS requires computational and storage resources to perform data warehousing, real-time processing, and model retraining. The initial cost can be a challenge for small organizations.
- **Privacy Concerns -** Data on user activity with threat intelligence may raise data-protection concerns, which need to be tightly governed and managed [12].

To address these limitations, both technical solutions (e.g., data cleaning automation, lightweight ML models) and organizational ones (e.g., governance structures, privacy policies) will be needed.

6.5 Possible Cost–Benefit Analysis

Building on these considerations, although the specific cost savings will vary in each organization, Table 3 presents a hypothetical cost-benefit analysis comparing the baseline IDS with the proposed BI-ML IDS. It points out that the shortening of incident-response time and the decrease in the number of false positives can also translate into a real financial value.

Table 3. Hypothetical Cost–Benefit Analysis of Baseline vs BI–ML IDS.

Metric	Baseline IDS	BI–ML IDS (Proposed)
Average detection rate	80 %	95 %
False-positive alerts per month	5,000	1,500
Analyst time spent on false positives (hrs/month)	400 hrs	120 hrs
Estimated annual loss from breaches (USD)	$2.5M	$0.8M
Estimated annual operational cost (USD)	$0.6M	$0.9M
Net annual savings (USD)	—	$1.2M

Despite the fact that the proposed system costs more to operate (because of infrastructure and model maintenance), the net saving is large as the breach-related losses and workload of the analysts are reduced. This is consistent with the recent research results that indicated that BI-enabled security analytics could enhance cybersecurity investments in terms of ROI [8], [18].

6.6 Synthesis and Future Directions

This discussion highlights the potential transformation of the combination of BI and ML-driven IDS. The framework, by addressing both technical and organizational aspects of cybersecurity, transforms intrusion detection into an active field, rather than merely responding to a threat.

Future studies need to concentrate on:

- Creation of automated quality-data-assessment tools of BI pipelines into IDS models.
- Employing explainable AI methods adapted to showcase a security dashboard to promote the concept of transparency.
- In response to cost-benefit assertions, conduct large-scale field experiments across various industries.

VII. FUTURE DIRECTIONS

Automated intrusion detection, achieved through the integration of Business Intelligence (BI) with AI-based Machine Learning (ML), represents a significant step towards proactive cybersecurity. As cyber threats become more sophisticated, advancing this research structure is increasingly vital. The following sections discuss how emerging technologies—such as large language models (LLMs), federated learning, and edge computing—offer opportunities for more adaptable, scalable, and privacy-preserving Intrusion Detection Systems (IDS) in the coming years.

7.1 Threat Intelligence Based on Large Language Models (LLMs)

Building on this, large language models (LLMs) offer new capabilities for threat intelligence. GPT-class LLPAs can handle large-scale unstructured text data, such as security logs, vulnerability feeds, and dark web threat reports. Future IDS solutions can offer more contextual awareness of possible attacks by integrating natural language understanding based on LLM with BI dashboards. For example, an IDS may automatically generate threat advisories or incident response reports and map them to potential network vulnerabilities, enabling real-time risk prioritization. This extends signature or anomaly detection by adding semantic reasoning—a feature that rule-based or traditional ML IDSs do not have.

7.2 Federated Learning of Privacy-Preserving IDS Models

Turning to another aspect, privacy and regulatory concerns continue to challenge data aggregation for IDS training. The majority of deployed IDS systems today face issues with sensitive network information that cannot always be aggregated due to privacy and regulatory constraints. Federated learning (FL) addresses this issue by enabling model training through decentralized nodes, avoiding direct data sharing. Future IDS frameworks can use FL to collaboratively train global ML models across organizations, sectors, or geographic areas while retaining proprietary or sensitive data on-premises. This approach enhances detection accuracy by learning from diverse threat landscapes while preserving privacy and adhering to regulations such as the GDPR.

7.3 Edge Cleaning of Instantaneous Intrusion Response

In parallel, another frontier emerges from the proliferation of IoT devices and distributed networks: latency is becoming a key concern in identifying and countering intrusions. Conventional IDS models that rely on central processing can experience delays, providing attackers with opportunities to exploit vulnerabilities. Deploying IDS components closer to network gateways or smart sensors, utilizing edge computing, significantly reduces detection and response times. Together with BI dashboards, this enables security analysts to access actionable intelligence almost in real-time, even within large, distributed environments.

7.4 Cross-Domain Threat Intelligence and Adaptive Learning

Looking beyond individual networks, the importance of cross-domain threat intelligence sharing is also growing. Facilitated with standards like STIX/TAXII, this will be especially valuable for future IDS systems. Combined with adaptive learning algorithms and LLM-assisted data enrichment, IDSs can shift from reactive to predictive defense. This emerging approach enables security teams not only to prevent intrusions but also to predict new attack vectors, simulate potential breaches, and implement automated mitigation measures within the BI context.

7.5 To Autonomous Decision-Making

Ultimately, integrating BI, ML, and these emerging technologies may result in IDS platforms evolving into semi-autonomous systems. Such systems will be able to suggest, prioritize, and even execute defensive actions. As a result, cybersecurity teams could spend less time on mean time to detect (MTTD) and mean time to respond (MTTR), focusing more on higher-order tasks such as policy design and compliance.

VIII. CONCLUSION

This paper proposes and evaluates a hybrid framework for integrating Business Intelligence (BI) and AI-powered machine learning (ML) to develop next-generation Intrusion Detection Systems (IDSs). This approach bridges the gap between traditional rule-based IDS and modern data-driven analytics, directly addressing deficiencies in detection accuracy, scalability, and decision support.

The results show that integrating BI layers into ML-based IDS significantly improves detection rates and transforms raw security data into actionable insights for real-time decision-making. The proposed system outperformed the baseline IDS in terms of precision, recall, F1-scores, and demonstrated lower false-positive rates. BI dashboards further enabled teams to contextualize alerts, prioritize risks, and allocate resources efficiently—meeting the urgent demands of today's evolving threat landscape.

A second contribution is the conceptual framework detailing how BI data pipelines feed ML algorithms, producing adaptive and context-rich intrusion detection. This architecture eliminates siloed analytics, creating a unified environment for proactive cybersecurity management. The comparative analyses and visualizations presented in the results confirm that this integrated approach is both effective and feasible.

The paper also identifies longer-term challenges, including data privacy, integration complexity, and the necessity of high-quality training data. These recognized barriers suggest directions for future research, such as private model training with federated learning, unstructured threat intelligence analysis using large language models (LLMs), and ultra-low-latency detection in distributed networks with edge computing. Advancing these areas may accelerate the shift from reactive to predictive and autonomous IDS.

The integration of BI and AI-based ML models marks a paradigm shift in intrusion detection. The framework proposed here not only enhances IDS technical performance but also adds strategic value for organizations securing critical infrastructure. By aligning analytics with actionable insights, this strategy enables security teams to transition from mere detection to the automated understanding and mitigation of attacks. This work supports a broader view of cybersecurity as a driver of organizational resilience, rather than just a tactical function.

REFERENCES

[1] Anshari, M., Syafrudin, M., Tan, A., Fitriyani, N. L., & Alas, Y. (2023, January 1). Optimisation of Knowledge Management (KM) with Machine Learning (ML) Enabled. Information (Switzerland). MDPI. https://doi.org/10.3390/info14010035

[2] Al-khateeb, B. A. A. (2024). Business Intelligence (BI). International Journal of Asian Business and Information Management, 15(1), 1–15. https://doi.org/10.4018/ijabim.340387

[3] Chen, Y., & Lin, Z. (2021). Business Intelligence Capabilities and Firm Performance: A Study in China. International Journal of Information Management, 57. https://doi.org/10.1016/j.ijinfomgt.2020.102232

[4] Dutt, I., Borah, S., &Maitra, I. K. (2020). Immune System Based Intrusion Detection System (IS-IDS): A Proposed. IEEE Access, 8, 34929–34941. https://doi.org/10.1109/ACCESS.2020.2973608

[5] Eskandari, M., Janjua, Z. H., Vecchio, M., &Antonelli, F. (2020). Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices. IEEE Internet of Things Journal, 7(8), 6882–6897. https://doi.org/10.1109/JIOT.2020.2970501

[6] Fachri, B., &Harahap, F. H. (2020). SimulasiPenggunaan Intrusion Detection System (IDS) SebagaiKeamananJaringandanKomputer. JURNAL MEDIA INFORMATIKA BUDIDARMA, 4(2), 413. https://doi.org/10.30865/mib.v4i2.2037

[7] Haleem, A., Javaid, M., AsimQadri, M., Pratap Singh, R., &Suman, R. (2022, January 1). Artificial intelligence (AI) applications for marketing: A literature-based study. International Journal of Intelligent Networks. KeAi Communications Co. https://doi.org/10.1016/j.ijin.2022.08.005

[8] Hamidinava, F., Ebrahimy, A., Samiee, R., &Didehkhani, H. (2023). A model of business intelligence on cloud for managing SMEs in COVID-19 pandemic (Case: Iranian SMEs). Kybernetes, 52(1), 207–234. https://doi.org/10.1108/K-05-2021-0375

[9] Işik, Ö., Jones, M. C., &Sidorova, A. (2013). Business intelligence success: The roles of BI capabilities and decision environments. Information and Management, 50(1), 13–23. https://doi.org/10.1016/j.im.2012.12.001

[10] Isik, O., Jones, M. C., &Sidorova, A. (2011). BUSINESS INTELLIGENCE (BI) SUCCESS AND THE ROLE OF BI CAPABILITIES. Intelligent Systems in Accounting, Finance and Management, 18(4), 161–176. https://doi.org/10.1002/isaf.329

[11] Jarrahi, M. H., Askay, D., Eshraghi, A., & Smith, P. (2023). Artificial intelligence and knowledge management: A partnership between human and AI. Business Horizons, 66(1), 87–99. https://doi.org/10.1016/j.bushor.2022.03.002

[12] Mannuru, N. R., Shahriar, S., Teel, Z. A., Wang, T., Lund, B. D., Tijani, S., … Vaidya, P. (2023). Artificial intelligence in developing countries: The impact of generative artificial intelligence (AI) technologies for development. Information Development. https://doi.org/10.1177/02666669231200628

[13] Mudau, T. N., Cohen, J., &Papageorgiou, E. (2024). Determinants and consequences of routine and advanced use of business intelligence (BI) systems by management accountants. Information and Management, 61(1). https://doi.org/10.1016/j.im.2023.103888

[14] Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. Computers and Security, 135. https://doi.org/10.1016/j.cose.2023.103525

[15] Oslejsek, R., Rusnak, V., Burska, K., Svabensky, V., Vykopal, J., &Cegan, J. (2021). Conceptual model of visual analytics for hands-on cybersecurity training. IEEE Transactions on Visualization and Computer Graphics, 27(8), 3425–3437. https://doi.org/10.1109/TVCG.2020.2977336

[16] Ozkan-Okay, M., Samet, R., Aslan, O., & Gupta, D. (2021). A Comprehensive Systematic Literature Review on Intrusion Detection Systems. IEEE Access. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2021.3129336

[17] Patil, S., Varadarajan, V., Mazhar, S. M., Sahibzada, A., Ahmed, N., Sinha, O., … Kotecha, K. (2022). Explainable Artificial Intelligence for Intrusion Detection System. Electronics (Switzerland), 11(19). https://doi.org/10.3390/electronics11193079

[18] Rehman, M. U., Ullah, R., Allowatia, H., Hasan, T. N., Perween, S., Ain, Q. U., &Ammad, M. (2023). Elaborating the Role of Business Intelligence (BI) in Healthcare Management. Journal of Intelligence Studies in Business, 12(2), 26–35. https://doi.org/10.37380/JISIB.V12I2.952

[19] Rahmani, A. M., Yousefpoor, E., Yousefpoor, M. S., Mehmood, Z., Haider, A., Hosseinzadeh, M., & Ali Naqvi, R. (2021, November 1). Machine learning (Ml) in medicine: Review, applications, and challenges. Mathematics. MDPI. https://doi.org/10.3390/math9222970

[20] Ramadhan, H. F., Fauzi, A., Rupelu, C. N., Aprillia, D. P., Anjani, N. D., &Halimatusadiah. (2022). Pengaruh Business Intelligence Terhadap Perusahaan DalamPengambilanKeputusan : Business Intelligence , Arsitektur Bi Dan Data Warehouse (KajianStudi Business Intelligence). JEMSI (JurnalEkonomiManajemenSistemInformasi), 3(6), 639–644. Retrieved from https://www.dinastirev.org/JEMSI/article/download/1105/668

[21] Singh, A., Prakash, J., Kumar, G., Jain, P. K., & Ambati, L. S. (2024). Intrusion Detection System: A Comparative Study of Machine Learning-Based IDS. Journal of Database Management, 35(1). https://doi.org/10.4018/JDM.338276

[22] Su, J., &Zhong, Y. (2022). Artificial Intelligence (AI) in early childhood education: Curriculum design and future directions. Computers and Education: Artificial Intelligence, 3. https://doi.org/10.1016/j.caeai.2022.100072

[23] SafanaHyder Abbas, Wedad Abdul KhuderNaser, &Amal Abbas Kadhim. (2023). Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Global Journal of Engineering and Technology Advances, 14(2), 155–158. https://doi.org/10.30574/gjeta.2023.14.2.0031

[24] Sun, P., Liu, P., Li, Q., Liu, C., Lu, X., Hao, R., & Chen, J. (2020). DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system. Security and Communication Networks, 2020. https://doi.org/10.1155/2020/8890306

[25] Talaoui, Y., Kohtamäki, M., &Rajala, R. (2020). Seeking “strategy” in business intelligence literature: Theorizing BI as part of strategy research. Technology Innovation Management Review, 10(9), 27–37. https://doi.org/10.22215/TIMREVIEW/1387

[26] Vanin, P., Newe, T., Dhirani, L. L., O’Connell, E., O’Shea, D., Lee, B., & Rao, M. (2022, November 1). A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning. Applied Sciences (Switzerland). MDPI. https://doi.org/10.3390/app122211752

[27] Vaishya, R., Javaid, M., Khan, I. H., & Haleem, A. (2020). Artificial Intelligence (AI) applications for COVID-19 pandemic. Diabetes and Metabolic Syndrome: Clinical Research and Reviews, 14(4), 337–339. https://doi.org/10.1016/j.dsx.2020.04.012

[28] Wang, J., Omar, A. H., Alotaibi, F. M., Daradkeh, Y. I., &Althubiti, S. A. (2022). Business intelligence ability to enhance organizational performance and performance evaluation capabilities by improving data mining systems for competitive advantage. Information Processing and Management, 59(6). https://doi.org/10.1016/j.ipm.2022.103075

[29] Yang, L., Moubayed, A., &Shami, A. (2022). MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles. IEEE Internet of Things Journal, 9(1), 616–632. https://doi.org/10.1109/JIOT.2021.3084796
[30] Zhao, Y., & Liu, Q. (2023). Causal ML: Python package for causal inference machine learning. SoftwareX, 21. https://doi.org/10.1016/j.softx.2022.101294