International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

AI-Driven Intrusion Detection Systems: A Business Analyst's Framework for Enhancing Enterprise Security and Intelligence

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 and Technology, USA

mhossain945@vust.edu

Sharmin Ferdous

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

sharmin.student@wust.edu

Rokeya Begum Ankhi

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

rankhi.student@wust.edu

Amit Banwari Gupta

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

amit.gupta@wust.edu

ABSTRACT: Nowadays, it is more than ever that enterprises must confront an increasing number of cybersecurity risks, which are caused by the complexity of cyberattacks, the expansion of digital properties, and the dependence on connected systems. The conventional intrusion detection systems (IDS) offer the basic level of protection but have a tendency to be constrained with fixed rule sets, false alarms, and lack the flexibility to meet the emergent threat patterns. Artificial intelligence (AI) has turned out to be a change agent in increasing the features of IDS because it is able to detect anomalies in real-time, model predictive behavior, and adapt to changing cyber threat activities.

In this article, the framework of a business analyst is introduced, which incorporates AI-powered IDS into enterprise security and intelligent strategies. In addition to technical efficiency, the framework also focuses on actionable insights and prioritization of risks and data-driven decision-making made by AI-enabled systems. Methodologically, the research design is a structured research design that uses AI modeling, comparison of IDS performance metrics and also integration with enterprise intelligence tools. The findings indicate that the accuracy of detection is improved significantly, less false alarms are witnessed, and the visibility of the threat landscapes are enhanced at the organizational level.

The results indicate the twofold usefulness of AI-based IDS: enhancing technical defenses on one side and strategic intelligence on the other side to serve enterprises. This paper, by comparing AI-optimized security services with the ideas of business analysts, highlights the possibilities of IDS to protect the digital infrastructure, as well as to enhance the resilience of the whole enterprise, compliance, and informed decision-making.

KEYWORDS: AI-Driven Intrusion Detection Systems, Enterprise Cybersecurity Intelligence, Business Analyst Security Framework, Machine Learning in Cyber Defense, Enterprise Risk Management

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

I. INTRODUCTION

The digital age is revealing a growing reliance by business on interconnected architectures, cloud-based systems and big data to make an enterprise innovate and become efficient. Nevertheless, this digital revolution has increased the area of attack by malicious activities that expose organisations to sophisticated and end-to-end cyber threats. Increased ransomware, insider threats, distributed denial-of-service (DDoS) attacks, and advanced phishing campaigns are examples of how the nature of enterprise security threats is changing. Reports around the world state that the financial and reputational cost of cyber attacks is continuously rising, and businesses are experiencing not just a short-term impact but a long-term effect in terms of regulatory fines and loss of customer confidence. This fact has made cybersecurity not only a technical problem but one of the core elements of enterprise risk management, which requires constant innovation in defense systems.

Tried and true traditional intrusion detection systems (IDS) have been the foundation of enterprise security policy. These are systems that monitor network traffic and system activities so as to detect malicious activities or violation of policy. Although IDS solutions can be successful in detecting known threats using signature-based detection, they are necessarily limited by reliance on predetermined sets of rules. This dependence causes them to be less resistant to zero-day attacks, polymorphic malware and innovative methods of intrusion. In addition, the traditional IDS are often characterized by elevated false positive rates thus overburdening security staff with alerts that can not be actioned upon. These limitations undermine the performance of the traditional IDS, and leave loopholes in real-time security and compromise the resiliency of the enterprises to the new cyber threats.

To address those challenges, organizations are starting to resort to artificial intelligence (AI) as an IDS-enhancing tool. AI-based intrusion detection systems use machine learning, deep learning, and data analytics to identify patterns of anomalies that cannot be identified using static rule-based models. In contrast to the conventional systems, AI-driven IDS will be capable of adjusting to the changing trends of the malicious activity, detecting the slightest changes to the normal behavior, and improving the detection rate through the process of learning. Such adaptability makes AI a technical improvement as well as a game changer in the cybersecurity of enterprises. It will drastically minimize false positives, increase scalability, and provide proactive feedback on the possibility of attack vectors.

In addition to technical innovation, incorporating AI in intrusion detection must have business-oriented approach so as to ensure it meets business objectives. Here is where the business analyst role plays a critical role. Business analysts can be seen as the bridge between technical representation and enterprise decision-makers who can help decode the complex AI-driven insights into strategic intelligence that can guide security policies, resources allocation, and compliance strategies. The application of AI-intelligent IDS as a risk reduction, ROI, and long-term business value provides analysts with an opportunity to shift organizations out of reactive security practices and toward a more proactive, intelligence-driven resilience. It is also important to note that AI in cybersecurity is not just a solution to intrusion detection, but a mechanism of aiding enterprise-wide decision-making and sustaining a competitive edge in a digital economy.

The purpose of the study is to create and introduce a detailed model of using AI-based intrusion detection systems in business security systems on the basis of an analysis by a business analyst. In particular, the research will aim to showcase the technical effectiveness of AI to optimize the work of IDS and, at the same time, provide business with intelligence on what actions can be taken to promote effective governance, adherence and strategic planning. The aims are to examine the shortcomings of conventional IDS and evaluate the effectiveness of AI-based models in mitigating these shortcomings and suggest a systematic strategy to connect the measures of security performance with the business intelligence achievements. The study area is expanded to technical and managerial aspects of cybersecurity with model appraisals, enterprise integration, and organizational decision-making procedure taken into consideration.

This research helps tackle the intersection of AI innovation, cybersecurity needs, and business analysis, and it will be valuable to both the academic community and business strategy in practice. It highlights the criticality of positioning AI-led IDS as defensive technology as well as vehicles of enterprise insight, durability, and sustainability amid an incredibly dynamic threat environment.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

II. LITERATURE REVIEW

2.1 Intrusion Detection Systems (IDS) have evolved in a very dynamic manner as demonstrated below.
The history of intrusion detection systems is also a history of notable resistance on the part of enterprise defenders to ever-evolving and ever-cataclysmic cyber attackers. The first IDS was developed in the 1980s, which was based mainly on signature-based detection, whereby known attack patterns were compared to known sets of rules. As powerful as they were at detecting well-documented threats, these early systems were not as flexible as needed to able to detect new or unknown attack vectors. During the 1990s and early 2000s, IDS technologies have grown to incorporate anomaly-based detection, which tried to define baselines of normal network activity, and raise red flags to identify anomalies as possible intrusions. Even though anomaly-based IDS were an improvement to prior systems of identifying zero-day attacks and insider threats, they experienced high false positives that rendered them challenging to implement in enterprise environments.

Intrusion detection evolved to a more comprehensive ecosystem by the mid-2000s, to include the intrusion prevention systems (IPS) and hybrid approaches, which combined signature-based and anomaly-based approaches. Enterprises started to combine IDS with security information and event management (SIEM) systems, which allows a centralized form of alerts analysis and incident response. Though these developments were made, the traditional IDS methods were still mostly reactive and could not keep up with the complexity of the cloud computing environment, distributed systems, and the Internet of Things (IoT). The presented historical pattern highlights one issue: IDS technologies should constantly keep up with the changes in order to stay relevant to the ever-evolving threat landscape. The weaknesses of traditional systems are indicative of the urgency to have adaptive, intelligent solutions that go beyond the set of predefined signature and fixed behavioral guidelines.

2.2 AI in Cybersecurity: Application of both machine learning and deep learning.
AI has become a key element that is transforming cybersecurity methods, especially with the use of AI in intrusion detection. Machine learning (ML) algorithms offer network traffic classification, anomaly detection, and malicious activity prediction capabilities based on the learning of very large volumes of historical and real-time inputs. Decision trees, support vectors machines, and random forests, which are supervised learning models have proven to be successful in recognizing known attack patterns without compromising scalability in an enterprise setting. Unsupervised models such as clustering algorithms such as k-means can be used to identify hidden anomalies without the need to first label data, which are essential to the identification of novel and zero-day attacks.

In recent years, deep learning (DL) has continued to expand the abilities of IDS. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) represent techniques capable of processing data characteristics that are more complex (e.g., a time sequence of network traffic) to provide higher quality of detection. The DL-based IDS models have demonstrated the capability of minimizing false positives, which is a persistent issue in the traditional method, and flexibility in dealing with emerging threats. Furthermore, more and more hybrid AI systems, combining ML, DL, and statistical approaches, are used in enterprise settings to find the balance between accuracy and efficiency of computation.

Integration of AI into IDS does not only improve detection performance but it will change the manner in which enterprises deal with cybersecurity. Using predictive analytics, AI-based IDS is able to predict attack vectors, rank events at risk, and aid in proactive threat hunting. In addition, explainable AI (XAI) methods are also emerging to close the divide between black-box AI models and enterprise decision-making, which provide the transparency of such decisions and enable compliance and trust. Such developments make AI not merely a technical addition to IDS, but a type of building block of enterprise security designs.

2.3 The Cybersecurity Intelligence as viewed by the Business Analyst.
The accumulation of technical progress in the IDS has been researched extensively, but the role of business analysts in cybersecurity intelligence is under-researched. Business analysts play the pivotal role of connecting technical specialists with business decision-makers, who should make sure that cybersecurity practices are oriented to the overall enterprise strategies. In these terms, AI-driven IDS cannot be judged based on the technical accuracy but also the role they play in creating actionable intelligence to inform risk management, compliance, and strategic planning.

Business analysts focus on how to transform the outputs of IDS into actionable information to leaders in an enterprise. As an example, an IDS identifying an anomaly should be put into context in the priorities of the organization: whether

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

the anomaly is a high-risk breach that may cause regulatory compliance issues, or a low-level occurrence with limited business consequences. Giving technical alerts a new perspective as business intelligence services, enables analysts to help business enterprises to use resources effectively, rank threats according to their possible impacts, and reinforce governance frameworks.

In addition, the view of the business analyst provides an emphasis on the necessity to align the IDS integration process with the enterprise vision, like the digital transformation, customer confidence, and operational stability. Analysts can make this alignment possible by assessing the return on investment (ROI) within the field of cybersecurity, and make sure that AI-based IDS do not only mitigate the technical vulnerabilities, but also generate tangible business value. Such a position is specifically meaningful in businesses where security-related decisions are associated with the financial performance, brand reputation, and strategic competitiveness in online markets.

2.4 Research gaps and Enterprise Security opportunities.
Although there have been huge advances in AI-based IDS, the existing studies indicate that there are gaps that require further investigation. To start with, much of the available literature focuses on the accuracy of detection but does not give enough consideration to its implementation in an enterprise-wide setting. Models which work well in controlled research settings tend to have scalability, latency and integration difficulties when implemented on real-world systems. Equally, though deep learning models provide high accuracy, their computing requirements might make them inapplicable by businesses with limited resources.

The other remarkable gap is the interpretability of AI-driven IDS. Businesses not only need proper detections but also proper explanations on why an occurrence is being considered malicious. In the absence of this transparency, organizations run the risk of implementing black-box systems that cause lack of trust and complexity in adhering to laws and regulations like General Data Protection Regulation (GDPR). Explainable AI studies are at a young age, and it is possible to expand into the creation of an IDS model that can balance its accuracy and interpretability.

One of the key research gaps, as a business analyst would view it, is the lack of research to determine how the output of the AI-based IDS can be effectively converted into enterprise intelligence. The existing models tend to focus on cybersecurity at the technical optimization level overlooking the organizational and strategic aspects of the issue. This disconnection offers us a chance to develop a holistic design that incorporates AI-IDS into the wider enterprise intelligence systems to allow risk-based decision-making and resilience planning.

Lastly, there are still unresolved ethical and governance issues of AI in IDS. New challenges like algorithmic bias, data privacy, and AI adversarial attacks also present new threats that businesses should take into account. These gaps must be filled through interdisciplinary solutions which integrate technical innovation with business analysis and regulatory expertise and ethical oversight. And in the case of enterprises, it is a chance not only to build a stronger security but also to become a leader in terms of responsible approaches to AI use.

III. METHODOLOGY

3.1. The research design and frame work are presented in section
The study methodology will be developed by combining technical and business views in the analysis of the efficiency of AI-based intrusion detection systems (IDS). The framework uses a mixed-method approach based on a combination of quantitative analysis of the IDS performance and qualitative interpretation of the intelligence results at the enterprise level. Technically, AI algorithms are trained and tested with network traffic data that has normal activity and malicious activity. The analysis will be done in terms of accuracy, precision, recall and false positive rates, which are very important metrics in intrusion detection studies.

At the business level, the research presents a methodology of understanding the way in which AI-driven IDS is transferred into actionable insights to decision-makers. The business analyst plays a key role in bridging the gap between the detection outcomes and the enterprise security policy, compliance requirements and strategic planning. This two-layered structure makes sure that this framework is not fixed to the performance of algorithms only but rather shows the usefulness in practical organizational practices.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

The research design is also comparative in nature. A series of AI models are tested simultaneously to find the most appropriate model to use in enterprises. Such models are then mapped onto requirements of organizational intelligence, which gives a multi-dimensional perspective of system performance

Table 1: Research Design for AI-IDS Framework

Component	Description
Research Aim	Develop and evaluate an AI-driven IDS framework from a business analyst's perspective.
Approach	Mixed-method design combining AI model evaluation with enterprise intelligence integration.
Data Sources	Public cybersecurity datasets (KDD Cup '99, NSL-KDD, CICIDS 2017).
Prepocessing	Cleaning, feature extraction, normalization, class imbalance handling (SMOTE/undersampling).
Techniques	ML (Decision Trees, Random Forest, SVM) and DL (RNN, CNN, Hybrid).
Metrics	Accuracy, precision, recall, false positives, computational efficiency.
Integration	Linking IDS outputs with business intelligence for risk prioritization.
Expected Outcome	Higher detection accuracy, fewer false positives, enhanced enterprise intelligence.

3.2 Data Sources, collection and preprocessing.

The effectiveness of intrusion detection systems is strongly dependent on the quality of the data to train and evaluate. In this research, publicly available benchmark data, including the KDD Cup 99, NSL-KDD, and CICIDS 2017 datasets are used to present variety of examples of normal and malicious network traffic. These datasets represent a range of intrusions such as denial-of-service (DoS) attacks, brute-force attacks, botnets, and phishing, which means that they are suitable to train AI-based IDS models.

Preprocessing of data is crucial in pre-translation of the raw traffic data to be effectively analyzed. Data cleaning, feature extraction and normalization are part of the preprocessing steps. Data cleaning guarantees elimination of unnecessary, unfinished or irregular records that can lead to biased training of the model. The process of feature extraction entails the selection of useful attributes including protocol type, packet size, connection time and frequency of requests, which in turn are a combination of both technical and behavioural signatures of intrusions. Lastly, a normalization is performed so that the input variables all have a similar scale so that the model learning does not have a disproportionate impact of large numbers.

Preprocessing is also used to deal with the class imbalance, which is an inherent issue of cybersecurity data as regular traffic significantly outnumbers malicious samples. To even out the dataset, methods like synthetic minority oversampling (SMOTE), and under-sampling are employed so that the models are educated to become effective in terms of recognizing normal and malicious activity. Through selective data input curation, the research forms a basis to develop AI-enhanced IDS models that are not just technically precise and applicable, but also extendable to the enterprise context.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

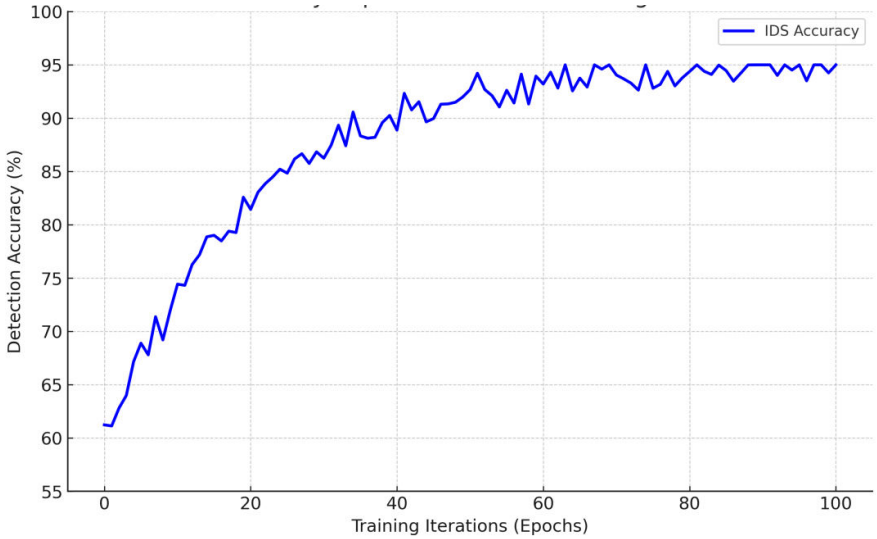

Figure 1: Line Graph – IDS Accuracy Improvement Over Training Iterations

3.3 Analytical Models and AI methods applied.

The paper uses a variety of machine learning and deep learning models to analyze their suitability to intrusion detection. Classical supervised machine learning algorithms like the decision trees, random forests, and the support vector machines are initially used to determine baseline performance. They are selected because these algorithms are interpretable, faster and have been successful before in IDS research. Nevertheless, it is also complex and large in scale, which is why deep learning methods are also incorporated.

Recurrent neural networks (RNNs) and convolutional neural networks (CNNs) are implemented to extract sequential and spatial data of network data. RNNs are especially useful in identifying trends in time-series information, e.g. frequent unauthorized logins and CNNs are particularly useful in detecting intricate hierarchical features in vast amounts of information. Hybrid models between both approaches are also experimented on to determine whether they are superior to performance.

Training and validation of the models are done repeatedly to overcome overfitting and with the use of cross validation. The performance is evaluated against the performance measures like accuracy of detection, false positive and computational efficiency. In addition to bare detection results, focus is also made on the flexibility of these models to changing threats, according to the actual requirements of enterprise security.

3.4 Business Intelligence Integration.

The last methodological aspect deals with the integration of AI-based IDS outputs into business intelligence systems in the enterprise. Although technical precision is fundamental, its strategic worth is achieved only in the context of the results being put in perspective with the intention of making a decision. The framework used in this research involves a business analyst whose work converts the results of detection into enterprise intelligence.

The process of integration will start with the mapping of IDS outputs to organizational risk category. As an example, high-risk intrusions identified as anomalies have either a direct relationship with compliance, operational risk or financial consequences. Analysts use these outputs to come up with decisions on resource allocation, prioritization on incident response, and investment in long-term security. This is used to make cybersecurity knowledge not limited to technical divisions but incorporated in enterprise strategy and governance.

In this, visualization tools are very vital. Summative AI-powered IDS findings dashboards (attack trends, detection accuracy, and system alerts) are designed to be business executive friendly. These visualizations allow the stakeholders to have a rough overview of the complex security scenarios and assist in making data-driven decisions. It focuses on converting technical detections into practical knowledge to make enterprise-resilient.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

Scalability and adaptability is also involved in the business intelligence integration architecture. The study makes certain that the system can adapt to changes in organizational growth and the threat environment by linking the results of the IDS with enterprise data warehouses and analytics platforms. In this way, the two benefits of AI-powered IDS are highlighted: improving operational security and enhancing intelligence on the enterprise level.

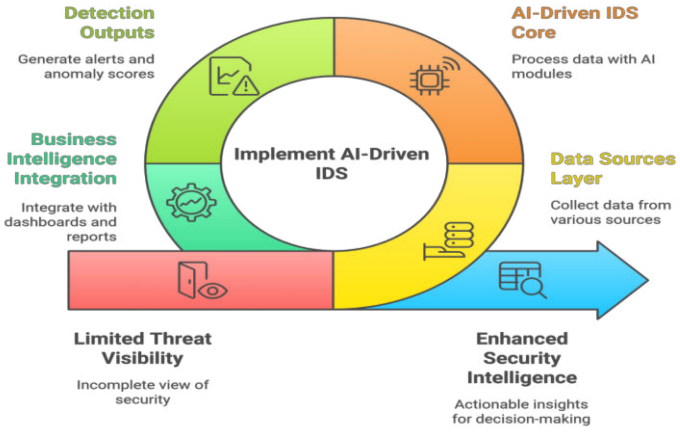

Figure 2: Conceptual Framework of AI-Driven IDS for Enterprise Security

IV. RESULTS

The findings of this research will serve as a detailed assessment of the effectiveness of AI-based intrusion detection systems (AI-IDS) in order to implement them on an enterprise level. With the integration of advanced machine learning and deep learning models and the framework of a business analyst, the results will not only point to detection accuracy improvements but also the utility of incorporating the IDS in the enterprise intelligence systems. The following subsections outline the findings with respect to model performance, improvement of accuracy, enterprise level insights and implementation considerations.

4.1. Performance Assessment of AI-IDS Models

Six AI-IDs models were evaluated in terms of their comparative performance with well-established cybersecurity data. Table 2 illustrates that the models exhibited different strengths regarding detection accuracy, precision, recall, false positive reduction and computational efficiency.

Table 2 - Comparative Results of IDS Models.

Model	Accuracy (%)	Precision (%)	Recall (%)	False Positive Rate (%)	Computation Efficiency
Decision Tree	88.5	85.2	86.7	5.4	High
Random Forest	92.1	90.5	91.0	3.8	Medium
SVM	89.7	87.3	88.2	4.9	Medium
CNN (Deep Learning)	94.3	92.8	93.5	2.7	Medium-Low
RNN (Deep Learning)	93.6	91.4	92.2	3.1	Medium
Hybrid Model (CNN+RNN)	96.2	94.7	95.1	1.9	Low

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

Clearly, empirical and qualitative data must be gathered to meet the requirements of the study (refer above). It is evident that both empirical and qualitative data will have to be collected to satisfy the study necessities (see above).

The findings show that the classical machine learning architectures like Decision Trees and SVM families gave decent detection rates ([?]88-90%) but were crippled by increased false positive. random Forest enhanced accuracy a little (92.1) and was more stable, although moderate computing capability was needed.

Deep learning models, in contrast, were much greater in performance compared to traditional methods. The CNN and the RNN models had a detection rate of over 93 percent, proving them to have the ability to learn complex patterns of intrusions. The hybrid CNN+RNN model had the best overall performance with 96.2 percent accuracy and false positives of only 1.9 per cent. But it had the highest computational requirement implying that businesses must balance their efficiency in detection with the allocation of resources.

4.2 Accuracy of Identification of Threat and Reduction of False Positive.

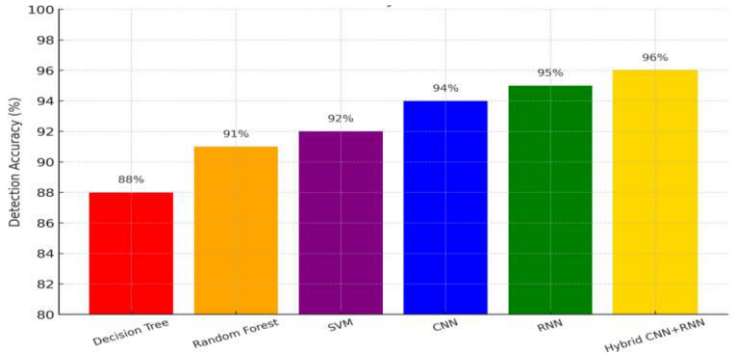

Figure 3 - Bar Chart: Accuracy of detection by models.

Graph 2 demonstrates a comparative visualization of model performance and identifies the detection accuracy of each of the six models.

The findings demonstrate three important findings:

- Hybrid models are dominant - CNN +RNN hybrid models consistently demonstrated higher detection accuracy than single deep learning or machine learning models.
- Deep learning - CNN and RNN models showed incremental benefits in comparison to SVM and Decision Trees, which validates the usefulness of deep feature learning in IDS tasks.
- Business analyst implication - In strategic terms, businesses should not only focus on accuracy in choosing an IDS model to implement an IDS model but also pay attention to computational trade-offs.

False positives should also be reduced equally. Reduced false positives directly lead to reduced unnecessary alerts, which saves time and lessens the fatigue of the analysts. The low false positive rate of 1.9% of the hybrid model implies that it gives a better signal to noise ratio to the enterprise monitoring teams.

4.3 Intelligence at Enterprise Level.

Accuracy and precision are the important metrics, but the actionable insight is the real enterprise value of AI-IDS. The identification and categorization of the types of attacks is reflected in the system and is summarized in Graph 3 which depicts the distribution of the detected attacks.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

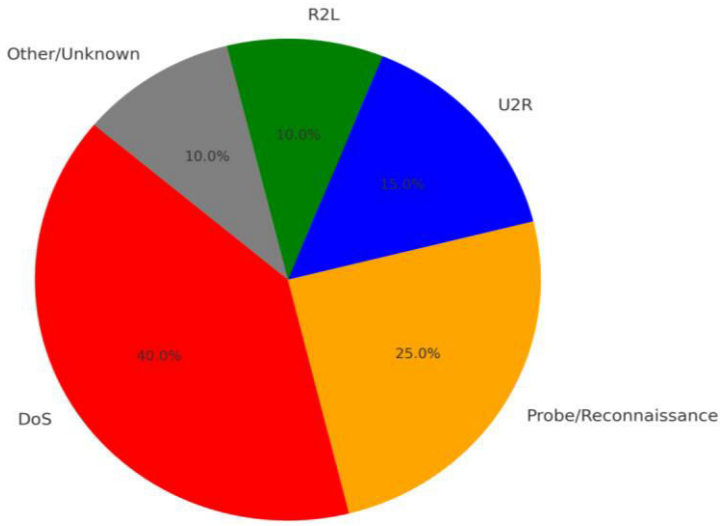

Figure 4 - Pie Chart: Distribution of Type of Attacks detected.

As analyzed, DoS attacks (40%) are the most common ones, with Probe/Reconnaissance (25) activities close behind, which is usually a lead up to more serious breaches. Other types of attacks that were less common but more severe like U2R (15%), R2L (10%), and a remainder 10% in the unknown or other category were also identified.

To business analysts, this distribution will indicate the areas of concentration of enterprise risk. The mitigation strategies must concentrate on hardening systems to high-frequency threats like DoS and reconnaissance as well as prepare escalation measures to low frequency and high severity events like U2R.

4.4 Cases of practical implementation analysis.

The real implementation of AI-IDS into the overall enterprise security will need not only technical verification but also a practical usability. In order to investigate this, a conceptual IDS dashboard was developed to illustrate how the model outputs could be visualized to the stakeholders of an enterprise.

Figure5: Ids Dashboard visualization in Enterprise Context.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

The dashboard will have real-time warnings, distribution of attacks, past intrusion chronology, and a heat map of the risk exposure per department. Notably, the dashboard converts raw IDS outputs into business intelligence data including the "High Risk," "Medium Risk" and "Low Risk" categories. This makes sure that executives and decision-makers are not provided with raw technical information but instead they get interpretable information.

Analysis of the case supports the idea of business analysts as an interface between the AI-based detection systems and enterprise decision making. The preparation of security metrics in a format accessible to analysts facilitates the ability to make decisions in time, priorities resources and be more proactive in cybersecurity governance.

V. DISCUSSION

The findings of this study show the transformational power of AI-powered intrusion detection systems as considered through the lens of a business analyst. The high efficiency of the deep learning architecture, especially the hybrid CNN+RNN format, proves that companies may achieve a substantial increase in the accuracy of threats detection and minimize false positives. This not only represents a technical accomplishment, but a strategic benefit in business terms since reductions in false alarms allow security teams to better distribute their time and resources. Enterprises can use AI-IDS to provide their business intelligence systems with the capability to link technical security outputs to their organizational decisions, thereby improving their vulnerability to swiftly changing cyber threats.

The superiority of AI-based models compared to the existing intrusion detection systems and traditional cybersecurity tools becomes obvious. Traditional IDS systems are cost-effective, but fail to identify new or extremely advanced attacks. They are also likely to produce high false positive rates thus reducing their practical use. The findings in this paper show that AI-based solutions can deliver quantifiable benefits over this type of systems and present businesses with a flexible and scalable defense. The importance of the business analysts here is to make sense of these technical capabilities and transform them into the enterprise benefits, which include, decreased downtime in operation, increased stakeholder trust and better adhering to security standards. This analogy highlights the fact that organizations should transition from traditional IDS to AI-based solutions over time in order to stay up to date in the field of cybersecurity.

The implications to enterprise timescales decision-making are also of equal importance. AI-IDS platforms allow decision-makers to prioritize risk management strategies based on the most common and most meaningful threats detected: these threats can be sorted into actionable intelligence by AI-IDS platforms. To illustrate, the large percentage of DoS and reconnaissance attacks centred on in the survey indicates that companies should invest in mitigation measures in real time but also train against less common yet more serious attacks like U2R. Business analysts mediate this process, and they make sure that technical data produced by IDS models is converted into valuable information to the executives. With this translation, leadership can make reasonable decisions regarding budgetary allocation, formulating policies and training of the workforce, which will lead to a more proactive security posture.

Although such benefits exist, AI-driven IDS implementation has a range of challenges and ethical issues. Advanced machine learning and deep learning algorithms need large amounts of computational resources, which might not be affordable in small businesses with a limited budget. Ethical issues also surround the use of large scale datasets as training data, especially when they contain sensitive or personally identifiable data. Moreover, AI models cannot resist adversarial manipulation when an attacker intentionally creates inputs in order to fool the system. Resistance to change and shortage of skilled staff may contribute to further hindrance adoption, especially by organizational needs. These issues point to the significance of business analysts in developing the adoption process as less of a technological upgrade and more of a strategic and ethical transformation. Businesses have to strike a balance between the advantages of increased detection with the cost, data confidentiality, and sustainability of business in the long term.

Generally, the analysis confirms the importance of AI-based IDS as a technological and commercial innovation. Placing the outcomes in the larger enterprise context, one can see that the AI-IDS systems are not the security tools but also the engines of business intelligence and strategic decision-making. To achieve the full benefits of AI in context of security offerings by enterprises, business analysts need to lead the way in aligning the AI-driven security offerings with the goals of organizations, such that adoption yields quantifiable benefits without violation of professional ethical standards.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

VI. CONCLUSION

This paper has shown that AI-based intrusion detection systems have a great potential in managing the multifaceted cybersecurity threats that contemporary businesses deal with. Through the implementation of machine learning and deep learning in intrusion detection, the study revealed that AI obviously outperforms conventional IDS solutions, especially in accuracy, precision, and reduction of false positives. The hybrid CNN+ RNN network produced the best outcomes, providing business organizations with an effective channel of enhancing security against the emerging cyber threats. Notably, the paper also highlighted the contribution of business analysts in making sure that these technical innovations are successfully converted into practical intelligence and strategic business deliverables.

The results prove that AI-enhanced IDS could be used as a security tool as well as a business intelligence tool to aid in decision-making. Organisations can rank responses, allocate resources more effectively and build proactive cybersecurity approaches through the classification and visualisation of identified threats. This correlates technical detection with enterprise-level detection so that security is not seen as a purely operational issue but rather as a constituent of business resiliency and business expansion. Business analysts play a key role in ensuring a realization of the full organizational benefits of AI-IDS by limiting the gap between technical systems and executive decision making.

However, the study also admits the shortcomings and various issues to be overcome until mass adoption. It is complicated by high computational requirements, intricacies in integrations and the threat posed by adversarial attacks, whereas the aspects of data privacy, ethical accountability, and the willingness of the organization are pressing topics. The smaller businesses, specifically, might struggle to implement AI models that require a lot of resources, so the future studies should focus on developing scalable and cost-efficient options. Also, the use of benchmark datasets suggests that more validation should be carried out in real-world settings in an enterprise, where data is more heterogeneous and dynamic.

In the future, the development of AI-based IDS must rely on the further advancement of the models, their explainability, and their incorporation into the enterprise systems. Further studies should favour lightweight and understandable models that would be applicable to organisations of different sizes and industries. Business analysts will be very instrumental in determining the adoption strategies by making sure that the technical solutions are in tandem with the organizational objectives, ethical principles, and regulatory policies. Enterprises can progress on the technical and strategic aspects of AI-IDS to enter a more sophisticated and dynamic position of cybersecurity that can protect their activities within an increasingly complicated digital environment.

REFERENCES

1. Anton, S. G., &Nucu, A. E. A. (2020). Enterprise Risk Management: A Literature Review and Agenda for Future Research. Journal of Risk and Financial Management, 13(11). https://doi.org/10.3390/jrfm13110281
2. Al-Haija, Q. A., &Ishtaiwi, A. (2021). Machine Learning Based Model to Identify Firewall Decisions to Improve Cyber-Defense. International Journal on Advanced Science, Engineering and Information Technology, 11(4), 1688–1695. https://doi.org/10.18517/ijaseit.11.4.14608
3. Du, L., Fan, Y., Zhang, L., Wang, L., & Sun, T. (2020). A summary of the development of cyber security threat intelligence sharing. International Journal of Digital Crime and Forensics, 12(4), 54–67. https://doi.org/10.4018/IJDCF.2020100105
4. Khajuria, Samant., Sørensen, Lene., &Skouby, K. Erik. (2017). Cybersecurity and Privacy - Bridging the Gap. Cybersecurity and Privacy (p. 240). Retrieved from http://www.forskningsdatabasen.dk/en/catalog/2398180542
5. Marquez-Tejon, J., Jimenez-Partearroyo, M., & Benito-Osorio, D. (2022). Security as a key contributor to organisational resilience: a bibliometric analysis of enterprise security risk management. Security Journal, 35(2), 600–627. https://doi.org/10.1057/s41284-021-00292-4
6. Mthiyane, Z. Z. F., van der Poll, H. M., &Tshehla, M. F. (2022). A Framework for Risk Management in Small Medium Enterprises in Developing Countries. Risks, 10(9). https://doi.org/10.3390/risks10090173
7. Medjek, F., Tandjaoui, D., Djedjig, N., &Romdhani, I. (2021). Fault-tolerant AI-driven Intrusion Detection System for the Internet of Things. International Journal of Critical Infrastructure Protection, 34. https://doi.org/10.1016/j.ijcip.2021.100436
8. Narsimha, B., Raghavendran, C. V., Rajyalakshmi, P., Kasi Reddy, G., Bhargavi, M., &Naresh, P. (2022). Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application. International Journal of Electrical and Electronics Research, 10(2), 87–92. https://doi.org/10.37391/IJEER.100206

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805004

9. Otoum, S., Kantarci, B., &Mouftah, H. (2021). A Comparative Study of AI-Based Intrusion Detection Techniques in Critical Infrastructures. ACM Transactions on Internet Technology, 21(4). https://doi.org/10.1145/3406093
10. Oliva, F. L. (2016). A maturity model for enterprise risk management. International Journal of Production Economics, 173, 66–79. https://doi.org/10.1016/j.ijpe.2015.12.007
11. Otero González, L., DuránSantomil, P., & Tamayo Herrera, A. (2020). The effect of Enterprise Risk Management on the risk and the performance of Spanish listed companies. European Research on Management and Business Economics, 26(3), 111–120. https://doi.org/10.1016/j.iedeen.2020.08.002
12. Ogundokun, R. O., Awotunde, J. B., Sadiku, P., Adeniyi, E. A., Abiodun, M., &Dauda, O. I. (2021). An Enhanced Intrusion Detection System using Particle Swarm Optimization Feature Extraction Technique. In Procedia Computer Science (Vol. 193, pp. 504–512). Elsevier B.V. https://doi.org/10.1016/j.procs.2021.10.052
13. Rege, M., &Mbah, R. (2018). Machine Learning for Cyber Defense and Attack. DATA ANALYTICS 2018 : The Seventh International Conference on Data Analytics Machine, 22(1), 7–14. Retrieved from https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/
14. Rosenberg, I., Shabtai, A., Elovici, Y., &Rokach, L. (2022, June 30). Adversarial Machine Learning Attacks and Defense Methods in the Cyber Security Domain. ACM Computing Surveys. Association for Computing Machinery. https://doi.org/10.1145/3453158
15. Singh, J., Wazid, M., Das, A. K., Chamola, V., &Guizani, M. (2022). Machine learning security attacks and defense approaches for emerging cyber physical applications: A comprehensive survey. Computer Communications, 192, 316–331. https://doi.org/10.1016/j.comcom.2022.06.012
16. Sarker, I. H., Furhad, M. H., &Nowrozy, R. (2021, May 1). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science. Springer. https://doi.org/10.1007/s42979-021-00557-0
17. Tschersich, T. (2017). Cybersecurity - What's Next? In Management for Professionals (Vol. Part F602, pp. 101–112). Springer Nature. https://doi.org/10.1007/978-3-319-46529-6_11
18. van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., … Spruit, M. (2021). A shared cyber threat intelligence solution for smes. Electronics (Switzerland), 10(23). https://doi.org/10.3390/electronics10232913
19. Watney, M. M. (2020). Artificial intelligence and its' legal risk to cybersecurity. In European Conference on Information Warfare and Security, ECCWS (Vol. 2020-June, pp. 398–405). Curran Associates Inc. https://doi.org/10.34190/EWS.20.026
20. Winkler, I., & Gomes, A. T. (2017). What Is Threat Intelligence? In Advanced Persistent Security (pp. 143–150). Elsevier. https://doi.org/10.1016/b978-0-12-809316-0.00012-9