Online ISSN
3007-3197
Print ISSN
3007-3189
http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 11 (2025)

An Efficient system based on Artificial Intelligence for the Detection and Mitigation of network Intrusion using encrypted traffic protocols: A Systematic Approach

[1*]Muhammad Waleed Khawar, [2]Nasir Ayub, Samra Shaheen, [3]Beenish Iftikhar, Hajra Masood, Ammar Ahmad, Hamayun Khan

Article Details

Keywords: Machine Learning, Deep Neural Network, CNN, Prediction models, Internet of Things, Threat Detection, Networks

Muhammad Waleed Khawar*
(Corresponding Author)
Department of Information Technology, Innova Networks, Lahore, 54000, Pakistan
waleedkhawar19@gmail.com
Nasir Ayub
Deputy Head of Engineering Calrom Limited, M16EG, United Kingdom
nasir.ayyub@hotmail.com
Samra Shaheen
Department of Information Technology, Innova Networks, Lahore, 54000, Pakistan
samrashaheen011@gmail.com
Beenish Iftikhar
Department of Computer Science, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan
beeenishiftikhar@gmail.com
Hajra Masood
Department of Computer Science, Bahria University Karachi Campus, Karachi, Pakistan
hajra.bukc@bahria.edu.pk
Ammar Ahmad
Department of Information Technology, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan
ammarahmed9917@gmail.com
Hamayun Khan
Department of Computer Science, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

ABSTRACT

Intrusion detection is a crucial aspect of cybersecurity, as attackers increasingly exploit encrypted traffic to conceal their malicious activities. While encryption enhances privacy and confidentiality, it also limits the effectiveness of traditional Intrusion Detection Systems (IDS), which primarily rely on inspecting the payload. Yet, these cut-edge technologies come with daily disastrous, ever-increasing cyberattacks on sensitive data in the IoT-based environment. Hence, there is a continued need for groundbreaking strengths of AI-based models to develop and implement intrusion detection systems (IDSs) to arras and mitigate these ugly cyber-threats with IoT-based systems. Therefore, this chapter discusses the security issues within IoT-based environments and the application of AI models for security and privacy in IoT-based for a secure network. The article proposes a hybrid AI-model framework for intrusion detection in an IoT-based environment using CIC-IDS2017and UNSW-NB15 to test the proposed model's performance. The model performed better with an accuracy of 99.45%, with a detection rate of 99.75%. The results from the proposed model show that the classifier performs far better when compared with existing work using the same datasets, thus proving more effective in the classification of intruders and attackers on IoT-based systems. Artificial Intelligence (AI)-based approaches to intrusion detection in encrypted network traffic, utilizing Machine Learning (ML) and Deep Learning (DL) methods that learn behavioral and statistical patterns, rather than relying solely on packet contents. Models such as Support Vector Machines (SVM), Random Forest (RF), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN) are examined in the context using standard datasets, such as CICIDS2017, NSL-KDD, and UNSW-NB15. The article shows the the strengths of these models, with a particular focus on scalability challenges, false positive rates, and adaptability in real-time encrypted environments. Furthermore, the study identifies critical research gaps, including the scarcity of updated encrypted datasets, the need for explainable AI (XAI) to enhance trust and transparency, and the potential of hybrid detection frameworks that combine host- and network-level perspectives. With the rise of cloud services, Internet of Things (IoT) devices, and virtualization technologies, the cyberattack surface has expanded significantly, creating more risks for organizations Overall, this article consolidates current approaches, emphasizes open challenges, and outlines future directions for developing efficient, scalable, and intelligent IDS capable of securing modern encrypted network

1. INTRODUCTION

Information and Communication Technology (ICT) systems have become the foundation of the digital age, supporting vital services in healthcare, finance, education, government, and business. These systems continuously handle sensitive and confidential data, making them highly attractive to cybercriminals and malicious insiders [1]. Attacks on ICT systems can be launched manually or automatically, and adversaries often use advanced techniques such as encryption, polymorphism, and obfuscation to bypass traditional defenses. The impact of these attacks is severe. For example, Yahoo's data breach led to losses of around $350 million, while a Bitcoin-related breach caused damages of nearly $70 million [2]. These developments underscore the pressing need for intelligent, adaptive, and scalable security mechanisms. One of the most widely used defense mechanisms in this context is the Intrusion Detection System (IDS) [3].. Encrypted traffic makes traditional Deep Packet Inspection (DPI) ineffective because the payload is hidden and cannot be analyzed directly. Instead of relying on content inspection, Artificial Intelligence (AI) techniques can detect threats by analyzing metadata features such as packet size, timing, and flow patterns, as well as temporal dependencies in traffic behavior. This shift highlights AI's role in providing adaptive detection in encrypted environments where conventional IDS approaches fail [4].

1.1 Intrusion Detection Systems (IDS) and Network-based IDS (NIDS)

Intrusion Detection Systems (IDS) are usually divided into two categories: Network-based IDS (NIDS) and Host-based IDS (HIDS) [5]. NIDS monitors network traffic passing through routers, switches, and firewalls, providing a comprehensive view of malicious activity. However, it faces challenges when most traffic is encrypted, since payloads cannot be inspected directly [6]. HIDS, in contrast, operates by monitoring activities on a specific host, including log files, system calls, and processes. While it provides detailed local visibility, it cannot identify large-scale or coordinated network attacks [7]. Due to these individual weaknesses, many modern enterprises rely on hybrid IDS architectures that combine NIDS and HIDS to provide both network-wide and host-level detection capabilities. IDS performance strongly depends on the detection strategy applied. The three most common techniques are signature-based, anomaly-based, and stateful protocol analysis [8]. A signature-based IDS functions by detecting intrusions through the comparison of current network activities with previously recorded attack signatures. They are highly accurate for detecting established threats, but fail against zero-day attacks or unknown malware. Anomaly-based IDS identifies potential intrusions by first studying the typical patterns of system behavior and then detecting any changes from these patterns as suspicious activity [9, 10]. Although this allows them to identify previously unseen threats, they often suffer from a high rate of false positives. Stateful protocol analysis evaluates traffic against predefined vendor specifications across multiple layers[11, 12]. This makes detection more accurate but requires considerable computational resources and an expert setup.

$$S_i^{(b,t)} = \sum_{z=1}^{E} p_{iz}^{(b)} J_z^{(b-1,t)} + \sum_{i'}^{y} x_{ii'}^{(b)} J_{i'}^{(b,t-1)} \qquad \text{Eq (1)}$$

Signature-based systems are precise when identifying already known threats, but their dependence on continuously updated signatures makes them less effective against novel or zero-day attacks. Anomaly-based systems, in contrast, are more adaptive, as they can recognize

unusual activities that may signal new forms of intrusion. However, their major drawback is the tendency to generate excessive false alarms, which reduces their reliability in practice[13, 14]. Table 1 illustrates that intrusion detection methods exhibit varying effectiveness depending on the type of attack and operational environment.

Table 1. Comparison of IDS Detection Approaches

Method	Strengths	Weaknesses	Applications	Ref
Signature-based	Accurate for known threats and low false alarms	Fails for zero-day attacks, and frequent updates are needed	Malware detection	[15]
Anomaly-based	Detects new/unknown intrusions	High false positives; resource-intensive	Emerging threats	[16]
Stateful Protocol Analysis	Multi-layer and protocol-aware detection	High computational cost; complex to deploy	Enterprise networks	[17]

Stateful protocol analysis offers a deeper and more structured view of traffic behavior, making it particularly suitable for enterprise-level networks where accuracy is crucial. At the same time, its demand for computational resources and configuration expertise makes it challenging to deploy widely. The comparison suggests that no single technique is sufficient on its own, and combining multiple approaches often yields stronger intrusion detection capabilities[18, 19].

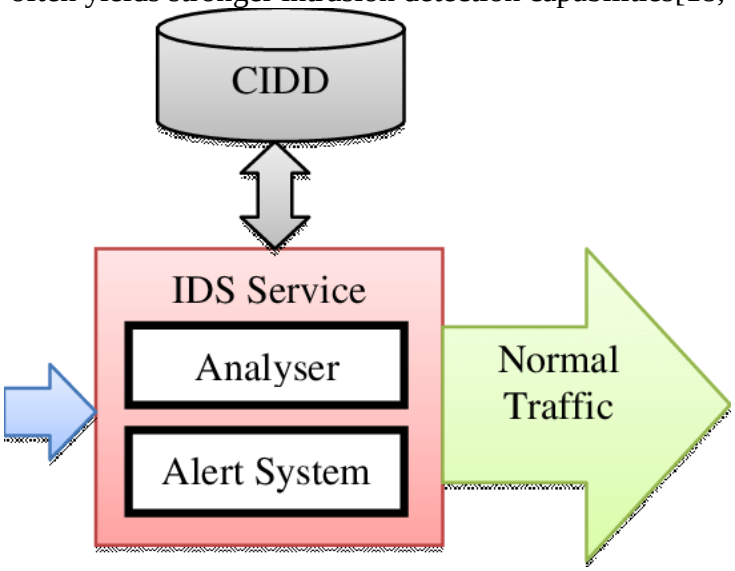


Figure 1. Evolution of IDS Approaches [20]

Figure 1 illustrates that an IDS service operates by analyzing incoming traffic with the aid of a knowledge base (CIDD) and then determining whether it is normal or malicious. The analyzer component inspects the data, while the alert system generates warnings if suspicious activity is detected. Traffic identified as legitimate is forwarded as everyday network communication, ensuring that harmful activities are filtered out before reaching the system. This structure highlights the fundamental workflow of IDS in separating safe traffic from potential threats [21].

$$J_i^{(b,t)} = \beta^{(b)}(S_i^{(b,t)})$$

Eq (2)

$$J^{(b,t)} = \beta^{(b)} \times (W^{(b)} \times J^{(b-1,t)} + W^{(b)} \times J^{(b,t-1)}) \quad \text{Eq (3)}$$

1.3 Impact of Encryption on IDS

The rapid growth of encryption protocols, such as TLS 1.3, QUIC, HTTPS, and DNS-over-HTTPS, has fundamentally reshaped the network security landscape, making intrusion detection increasingly complex and challenging [22]. Encryption is widely regarded as essential for ensuring confidentiality, data integrity, and user privacy in digital communication. It prevents eavesdropping and protects sensitive information such as financial transactions, personal records, and enterprise communications from being intercepted by adversaries. However, the exact property that makes encryption valuable also reduces the visibility of network monitoring tools. Traditional techniques, such as Deep Packet Inspection (DPI), which rely on analyzing the payload of packets, are no longer effective because the contents of encrypted streams remain hidden from inspection [23, 24].

$$\ln fl_{it}^{+} = \Sigma_{j=0}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \Sigma_{j=0}^{t} \max(\Delta W^{T}{}_{ij,0}) + \epsilon_{it} \quad \text{Eq (4)}$$

Attempting large-scale decryption to regain visibility is not a feasible solution. Decryption requires significant computational resources, which increase operational costs and introduce delays that can slow down communication [25]. Moreover, decrypting traffic at scale raises serious privacy concerns and may conflict with frameworks such as GDPR, HIPAA, or national data protection laws, making it unsuitable for real-world deployment. Consequently, researchers have shifted toward alternative strategies that do not require decryption [26, 27]. Metadata-based approaches, for example, analyze observable features like packet sizes, inter-arrival times, burst patterns, and flow durations.

$$\ln fl_{it}^{+} = \Sigma_{j=1}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \Sigma_{j=1}^{t} \max(\Delta W^{T}{}_{ij,1}) + \epsilon_{it} \quad \text{Eq (5)}$$

These indicators, although indirect, can reveal abnormal patterns of behavior that are often associated with malicious activities, such as botnet communications, tunneling, or denial-of-service attacks [28]. Table 2 illustrates the challenges encryption introduces for intrusion detection. While protocols like TLS 1.3, QUIC, VPN, and DoH/DoT enhance confidentiality and safeguard user privacy, they also limit the visibility of IDS tools by concealing packet payloads.

$$\ln fl_{it}^{+} = \Sigma_{j=2}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \Sigma_{j=2}^{t} \max(\Delta W^{T}{}_{ij,2}) + \epsilon_{it} \quad \text{Eq (6)}$$

As a result, IDS solutions must rely on indirect indicators such as packet sizes, timing patterns,

session duration, and flow characteristics.

$$B_{m,n}(q+1)(1-\frac{1-X(0,1)-X(-1,1)}{1-c_{m,n}\times f_{mn}(q)}) = X(0,1)\times R_{s,n} \quad \text{Eq (7)}$$

These features can reveal unusual communication behaviors, but they rarely provide the complete context required for accurate detection [29]. For instance, TLS 1.3 reduces access to handshake details, QUIC complicates stateful analysis, and VPNs completely mask internal traffic flows. Similarly, encrypted DNS queries prevent the identification of malicious domains through traditional DNS monitoring. The table highlights the trade-off between maintaining privacy and ensuring adequate security, underscoring the need for novel IDS strategies that balance both requirements [30].

Table 2. Encrypted Protocols and IDS Visibility

Method	Strengths	Weaknesses	Applications	Ref
Protocol	Visibility Challenge	Observable Features	IDS Limitation	[31]
TLS 1.3	Encrypts most handshakes; removes static keys	Packet size, timing, SNI (if visible)	Payload unavailable	[32, 33]
QUIC	Combines transport + crypto; supports 0-RTT	Flow RTT, burst size, initial packets	Hard to perform stateful analysis	[34]
VPN (SSL/IPsec)	Hides internal traffic in encrypted tunnels	Tunnel duration, byte counts, endpoints	No visibility into inner flows	[35, 36]
DoH/DoT	Encrypts DNS queries	Query cadence, request size	Blocks DNS-based threat detection	[37, 38]

1.4 Use of Artificial Intelligence in IDS

Artificial Intelligence (AI) has become a cornerstone in the evolution of Intrusion Detection Systems (IDS), providing innovative solutions to overcome the limitations of traditional detection techniques. Early approaches relied heavily on manually engineered features and statistical traffic analysis, which required significant domain expertise and often failed to generalize across diverse attack scenarios. With the introduction of Machine Learning (ML), algorithms such as Support Vector Machines (SVM), Random Forest (RF), Decision Trees (DT), and k-Nearest Neighbors (k-NN) were employed to identify types of network traffic by studying labeled datasets [39]. These models demonstrated improved detection performance compared to signature-based systems, particularly in identifying unknown or slightly modified attacks. However, they still depended heavily on feature engineering, which limited scalability and adaptability to new environments. The arrival of Deep Learning (DL) marked a significant turning point in IDS research. DL models are capable of automatically extracting hierarchical and hidden patterns from raw data, while reducing the need for manual feature design [40]. Convolutional Neural Networks (CNNs), for example, have been helpful to traffic classification by analyzing spatial dependencies in packet sequences. At the same time, Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) models are highly effective in modeling sequential and time-dependent patterns in traffic flows [41, 42]. More recently,

Transformer models that use self-attention techniques have been explored for their ability to capture contextual relationships across long sequences of data, making them suitable for detecting complex, multi-stage cyberattacks. Beyond network-level detection, AI has also been applied at the host level [43]. Natural Language Processing (NLP) techniques treat system calls or log data as sequences, enabling IDS to model program behavior similarly to language modeling, thereby improving detection of stealthy and process-level intrusions. Together, these AI-driven approaches demonstrate significant potential for adaptive, scalable, and intelligent intrusion detection [44].

1.5 Challenges in AI-Based IDS

While AI-driven IDS represents a significant leap forward, several unresolved challenges continue to hinder widespread adoption in real-world environments. One of the most persistent issues is the high number of false positives, where regular traffic is incorrectly identified as malicious. Excessive false alarms not only erode analyst trust but also overwhelm security teams, wasting resources on unnecessary investigations. Another major limitation arises from dataset dependency [45, 46]. Most IDS research relies on publicly available datasets, such as NSL-KDD, CICIDS2017, and UNSW-NB15. Although these datasets have supported benchmarking and comparative studies, they remain limited in scope and fail to capture the scale, encryption diversity, and constantly evolving nature of real-world traffic. As a result, models trained on these datasets often fight to simplify when deployed in live environments.

Scalability further complicates the deployment of AI-based IDS. Modern enterprise and IoT networks generate vast amounts of high-speed traffic, and many deep learning models lack the efficiency to process this data in real-time [47]. Resource constraints make it challenging to apply large DL architectures without significant hardware investments. Additionally, interpretability remains a pressing concern. Most deep learning models operate as “black boxes,” producing highly accurate outputs without providing clear explanations or justifications for their decisions. In a domain like cybersecurity, where accountability and explainability are crucial, this lack of transparency reduces the trust of security analysts and slows incident response [48, 49].

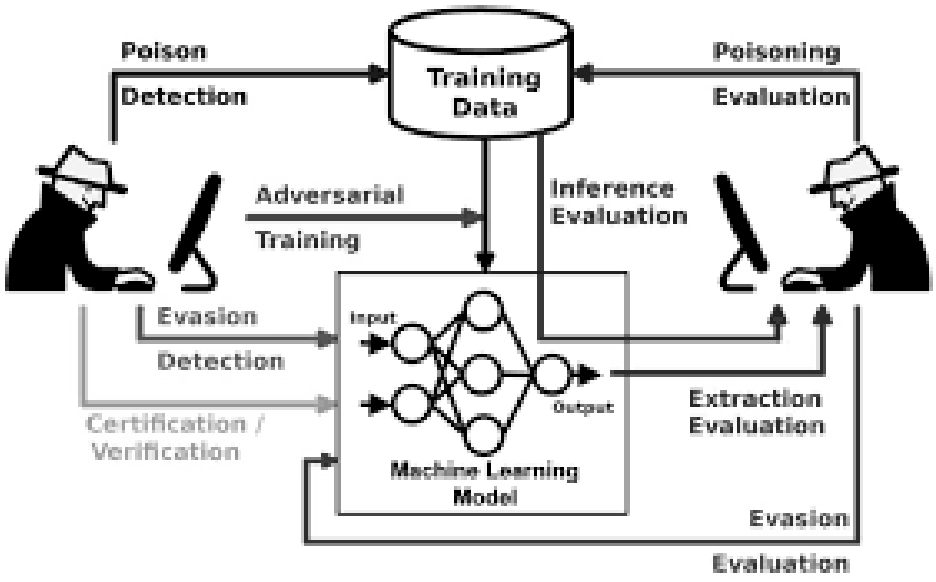


Figure 2. Workflow of AI-Based IDS [50].

Figure 2 illustrates the workflow of an AI-based IDS, showing how the model interacts with both

adversarial threats and defensive mechanisms. Attack vectors such as poisoning, inference, extraction, and evasion highlight the vulnerabilities of IDS, while countermeasures like poison detection, adversarial training, and certification strengthen its resilience. This framework emphasizes the ongoing balance between evolving cyberattacks and intelligent defense strategies. To address these barriers, researchers are exploring federated learning to reduce dataset dependency, transfer learning to use pre-trained models to new threats, and Explainable AI (XAI) to provide interpretability of model predictions [51, 52]. As shown in Table 3, several critical challenges hinder the effectiveness of AI-driven IDS, along with the strategies currently being explored to mitigate them. One of the most pressing issues is the high number of false positives, which reduces analyst trust and wastes valuable resources. Context-aware deep learning models address this by learning richer traffic patterns, thereby minimizing unnecessary alerts. Another limitation is dataset dependency, as most IDS models were trained on outdated or restricted datasets that failed to reflect the complexity of modern networks [53]. Federated and transfer learning approaches provide alternatives by enabling models to adapt to diverse environments without requiring centralized datasets. Scalability is also a key concern, as enterprise and IoT networks generate vast amounts of high-speed traffic that many deep learning models struggle to process in real-time. Parallel and distributed learning frameworks are being introduced to improve efficiency in such scenarios. Furthermore, encrypted traffic conceals payload information, but metadata-based feature learning offers partial visibility through flow-level characteristics [54]. Finally, the lack of interpretability in deep models limits analyst trust, a challenge being addressed through Explainable AI (XAI) techniques that make model outputs more transparent. Collectively, the table illustrates that while AI offers powerful tools for IDS, practical deployment requires addressing these ongoing challenges [55].

Table 3. Challenges in Encrypted Traffic Detection and AI-Based Solutions

Challenge	Limitations of Current IDS	AI-Based Solution	Ref
High false positives	Too many false alarms for analysts	Context-aware DL models reduce noise	[56]
Dataset dependency	Poor generalization across networks	Transfer learning and federated learning	[57]
Scalability	Struggles with high-speed flows	Parallel and distributed deep learning frameworks	[58]
Encrypted traffic	Hidden payloads, privacy concerns	Metadata-based feature learning	[59]
Interpretability	Models act as black boxes	Explainable AI (XAI) techniques	[60]

1.6 Hybrid and Comparative Approaches

Hybrid Intrusion Detection Systems (IDSs) have emerged as a promising solution to overcome the limitations of separate methods by combining the strengths of both Network-based IDS (NIDS) and Host-based IDS (HIDS) with advanced Artificial Intelligence techniques. Traditional NIDS provide wide visibility across network traffic, while HIDS offer detailed insights at the system level, such as monitoring processes, log activities, and system calls. By merging these two perspectives, hybrid IDS frameworks create a more holistic detection mechanism that can identify both external and internal threats with higher accuracy. A notable example of such integration is the Scale-Hybrid-IDS-Alert-Net (SHIA), which fuses host-level and network-level

data with deep learning algorithms to provide scalable, real-time detection of malicious activities [61, 62]. This distributed architecture enables SHIA to handle large volumes of traffic while maintaining detection accuracy, making it suitable for enterprise-level environments. In addition to structural hybrids, research has also explored the combination of different analytical methods. For instance, Natural Language Processing (NLP)-based IDS applied to host monitoring treats system calls as sequential patterns, allowing detection of stealthy intrusions that might otherwise bypass signature-based or anomaly-based techniques. Such methods highlight the value of cross-disciplinary approaches, where ideas from AI subfields, such as NLP or reinforcement learning, can be applied to cybersecurity challenges [63, 64]. To better understand the distinctions in analytical power and practical application, researchers have conducted comparative studies between classical Machine Learning (ML) and modern Deep Learning (DL) methods. ML models such as SVM and Random Forest provide interpretability and lower computational costs, but they often depend profoundly on feature engineering. Deep Learning models, such as CNNs, RNNs, and Transformers, on the other hand, can automatically extract features and capture complex spatial, temporal, and contextual dependencies in traffic flows, albeit at the cost of higher resource demands [65]. As presented in Table 4, machine learning (ML) and deep learning (DL) approaches in IDS each have distinct strengths and weaknesses. ML techniques such as SVM, Random Forest, and k-NN are valued for their efficiency, lower computational requirements, and interpretability, which makes them suitable for resource-constrained environments or scenarios where transparency is critical. However, their dependence on manually designed features restricts their effectiveness against modern, complex cyberattacks[66, 67]. On the other hand, DL models—including CNNs, RNNs, LSTMs, and Transformers—excel at automatically extracting spatial, temporal, and contextual features from raw traffic, allowing them to recognize complex attack patterns and encrypted threats with higher accuracy. Despite these advantages, DL approaches demand significant computational resources and often act as “black boxes,” as they do not clearly explain how they make decisions. This trade-off highlights a clear distinction: ML remains practical for smaller-scale or interpretable applications. At the same time, DL is more effective for large-scale, high-accuracy intrusion detection in modern network environments [68].

Table 4. Comparison of ML and DL Approaches in IDS

Approach	Example Models	Strengths	Weaknesses	Ref
ML	SVM, Random Forest, k-NN	Requires fewer resources; easy to interpret	Needs manual feature engineering; less effective on complex data	[69]
DL	CNN, RNN, LSTM, Transformers	Learns patterns automatically; handles large data	Requires more computation; low interpretability	[70]

Conventional IDS approaches, such as signature-based and anomaly-based detection, were practical in earlier, less complex environments; however, they now struggle to cope with the scale, diversity, and sophistication of modern cyberattacks. With more than 90% of global internet traffic expected to be encrypted, relying on payload inspection has become impractical, leaving organizations vulnerable to hidden attacks that pass through undetected. This reality underscores the urgent need for intelligent, AI-driven systems that can analyze encrypted traffic

while maintaining efficiency, accuracy, and compliance with privacy regulations. Evaluates benchmark datasets, such as CICIDS2017, UNSW-NB15, and ADFA-LD, identifying their strengths and weaknesses in terms of realism, scalability, and representativeness. Additionally, it examines the potential of hybrid IDS frameworks that combine both NIDS and HIDS, as well as the significance of explainable AI (XAI) in enhancing analyst trust and system transparency [71, 72]. By addressing persistent issues such as dataset dependency, scalability, false positive rates, and interpretability, this paper sets a direction for the next generation of IDS. In conclusion, while the dominance of encrypted protocols has weakened the effectiveness of traditional payload-based inspection, AI-based IDS, particularly those using hybrid and explainable models, offer a promising pathway. Despite ongoing challenges related to scalability, trust, and dataset diversity, the steady progress in ML, DL, and hybrid frameworks provides a strong foundation for building efficient and intelligent IDS capable of safeguarding modern digital infrastructure [73].

1.8 Paper Organization

The remainder of this paper is organized as follows. Section 2 presents a comprehensive literature review, tracing the evolution of intrusion detection systems from traditional approaches to AI-based methods, while also addressing the challenges posed by encryption, dataset limitations, and scalability issues. Section 3 outlines the methodology used in this review, including the selection criteria for studies, classification schemes, and evaluation metrics. Section 4 presents a comparative analysis of IDS approaches, supported by tables that summarize strengths, weaknesses, datasets, and performance results. Section 5 discusses key challenges, identifies research gaps, and highlights future research directions in AI-driven IDS. Finally, Section 6 concludes the paper by summarizing significant findings and outlining recommendations for the development of scalable, interpretable, and effective IDS solutions.

2. Literature Review

Research on Intrusion Detection Systems (IDS) has undergone a remarkable development over the last two decades, gradually shifting away from rule-based models to more advanced Artificial Intelligence (AI)-driven approaches. In the earliest stages, IDS were primarily based on signature detection, also known as misuse detection, where traffic was matched against a database of known attack signatures. These systems were highly reliable for detecting previously documented threats such as viruses, worms, and denial-of-service attacks. Their primary drawback was the failure to identify novel, unknown, or zero-day attacks. Any novel malware or attack technique that lacked a pre-existing signature could completely bypass detection, creating significant blind spots in security monitoring [74].

To address these shortcomings, researchers developed anomaly-based detection systems. Instead of relying solely on predefined attack patterns, anomaly-based IDS created models of “normal” network behavior and flagged any significant variations as possible intrusions.

$$MCC = \frac{TP * TN - FP * FN)}{\sqrt{((TP + FP) * (TP + FN) * (TN + FP) * (TN + FN))}} \qquad \text{Eq (8)}$$

This approach offered the significant benefit of identifying previously unseen attacks, making it more flexible than signature-based detection. However, anomaly-based detection also comes with particular challenges. It was often prone to generating high false positive rates, overwhelming security analysts with unnecessary alerts. In large-scale enterprise networks, this issue of false alarms limited their practical adoption, as organizations could not allocate

sufficient resources to investigate every flagged event [75].

$$f = -Ex\sim pdata\ [\log\ pmodel(x)] \quad \text{Eq (9)}$$

$$f(x,y,w) = -\log\ p(y|x;w) \quad \text{Eq (10)}$$

2.1 Development of Intrusion Detection Systems

The next stage of development was the introduction of stateful protocol analysis. Unlike previous methods, this approach examined communication across multiple protocol layers by cross-referencing predefined vendor specifications. It provided deeper visibility into network flows, allowing for more precise detection of protocol deviations and multi-stage attacks. Despite these improvements, stateful protocol analysis proved to be computationally expensive and resource-intensive, making it difficult to scale in high-speed, modern networks where massive amounts of data need to be analyzed in real-time. These limitations paved the way for the adoption of AI-based IDS, which offered more scalable and intelligent solutions to evolving cybersecurity threats [76].

2.2 Machine Learning Approaches in IDS

The integration of Artificial Intelligence (AI) represented an important milestone in the advancement of Intrusion Detection Systems (IDS). The first wave of AI adoption in this field was driven by Machine Learning (ML) algorithms, which enabled the detection of intrusions without relying on static attack signatures. Algorithms like Support Vector Machines (SVM), Random Forest (RF), Decision Trees (DT), and k-Nearest Neighbors (k-NN) were among the earliest applied to intrusion detection tasks. Unlike traditional signature-based IDSs that depend on predefined patterns, these ML models can analyze statistical and behavioral features of network traffic, allowing them to recognize subtle irregularities and generalize detection to a broader range of threats [77, 78].

Studies demonstrated that ML-based IDS could effectively distinguish between normal and malicious traffic, achieving greater adaptability compared to earlier systems. Benchmark datasets, such as KDDCup99 and its refined successor, NSL-KDD, have been widely used to train and test these models. These datasets enabled researchers to establish a foundation for ML in IDS, allowing comparative evaluations of algorithmic performance. For example, SVM was shown to perform well in classifying high-dimensional data, while Random Forest and Decision Trees offered interpretability and robustness against noisy inputs [79].

$$minw \in Rd\ f(w) = K \sum k=1\ nk\ n\ Fk(w) \quad \text{Eq (11)}$$

Lipschitz Objective Function (LOF): $f(x)$ is β-Lipschitz continuous if there exists

$\beta \geq 0$ such that for all $x1,x2 \in Rd$

$$|f(x1) - f(x2)| \leq \beta \|x1 - x2\|. \quad \text{Eq (12)}$$

Smooth Objective Function (SOF): $f(x)$ is L-smooth if f (x) has L-Lipschitz con- tinuous gradient, i.e., for all $x1,x2 \in Rd$,

$$\|\nabla f(x1) - \nabla f(x2)\| \leq L \|x1 - x2\| \quad \text{Eq (13)}$$

Strongly Convex Objective Function (SCOF): $f(x)$ is μ- strongly convex if there exists $\mu \geq 0$ such that for all $x1, x2 \in Rd, f(x1) \geq f(x2) + (x1 - x2)T\nabla f(x2) + \frac{\mu}{2}$

$$f(x1) \geq f(x2) + (x1 - x2)T\nabla f(x2 \quad \text{Eq (14)}$$

Coercive Function (CF): $f(x)$ is coercive if $\lim \|x\| \to \infty f(x) \to \infty$.

Bounded Variance (BV): The variance of each stochastic gradient $\nabla fi(x;\xi)$ is bounded if there exists $\sigma \in R$, such that

$$E\xi \|\nabla fi(x;\xi) - \nabla fi(x)\|2 \leq \sigma 2, \quad \text{Eq (15)}$$

Despite these advances, the reliance on outdated datasets quickly became a bottleneck for real-world deployment. Although valuable in their time, KDDCup99 and NSL-KDD faced criticism for containing redundant records, unrealistic traffic patterns, and limited variety in attack scenarios. Most importantly, these datasets did not capture the characteristics of modern encrypted traffic, where payload inspection is impossible. As a result, ML models trained on them often struggled to generalize to real-world network environments, highlighting the urgent need for more comprehensive datasets and leading towards the adoption of Deep Learning (DL)-based methods in IDS research [80, 81].

2.3 Rise of Encrypted Communication and Its Challenges

The widespread adoption of secure communication protocols, such as HTTPS, TLS 1.3, SSL, and VPN tunneling, has significantly reduced the visibility available to intrusion detection systems, making traditional deep packet inspection (DPI) far less effective [82]. In earlier generations of IDS, it was possible to inspect packet payloads directly and identify attack signatures embedded in the traffic. However, the growing reliance on encryption has made this practice nearly impossible. Since most packet contents are now concealed within encrypted streams, IDS solutions are unable to analyze the actual payload without first decrypting it. Large-scale decryption is not a practical solution, as it not only requires vast computational resources but also introduces latency into communications, violating privacy regulations such as the GDPR and HIPAA, which place strict limitations on how personal or sensitive data can be handled [83, 84].

This shift has forced researchers and practitioners to explore new techniques for maintaining security visibility in encrypted environments. Instead of relying on payload inspection, attention has turned toward metadata and traffic flow features that remain observable even when content is hidden. Characteristics such as packet size distribution, inter-arrival time, session duration, burst frequency, and statistical flow behavior can serve as indirect yet meaningful indicators of malicious activity. For instance, abnormal variations in packet length or sudden traffic spikes may suggest distributed denial-of-service (DDoS) attacks or botnet activity. At the same time, irregular timing patterns between sessions could reveal covert communication channels or tunneling attempts [85, 86].

The challenge, however, lies in ensuring that these metadata-based approaches are accurate and

adaptable. Attackers are becoming increasingly skilled at mimicking standard traffic patterns, making it more challenging for intrusion detection systems to distinguish between legitimate encrypted traffic and malicious flows. This has created a pressing need for advanced analytical techniques, particularly those powered by artificial intelligence, to extract deeper insights from limited observable features [87]. As a result, the effectiveness of IDS in encrypted environments is now closely tied to the sophistication of feature engineering and the ability of machine learning and deep learning models to recognize subtle, context-dependent anomalies. Additionally, the scalability of these techniques is a significant concern, as enterprise networks generate massive amounts of encrypted traffic that must be processed in real-time. Furthermore, privacy-preserving methods must be integrated to ensure that monitoring does not compromise user confidentiality while still enabling accurate intrusion detection. These combined challenges make encrypted communication one of the most critical areas driving innovation in IDS research today [88].

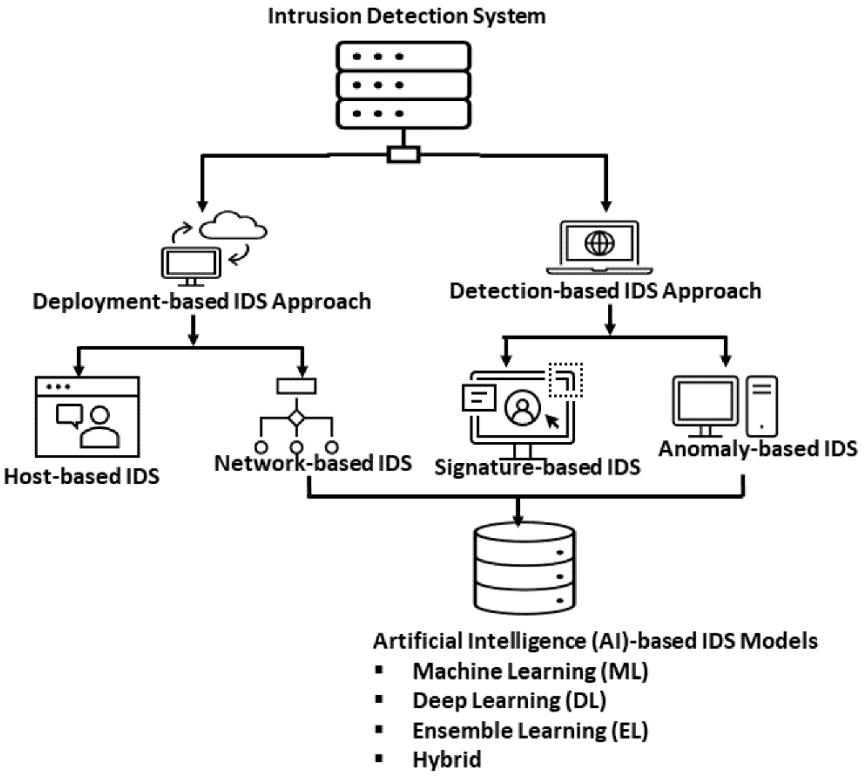


Figure 3. Hybrid AI-Based IDS for Encrypted Traffic [89]

Figure 3 illustrates the classification of Intrusion Detection Systems (IDS) based on deployment and detection strategies. In the deployment-based category, IDS can be either host-based or network-based, while detection-based systems are separated into signature-based and anomaly-based approaches. The figure also emphasizes the integration of Artificial Intelligence (AI)-driven models, including machine learning, deep learning, ensemble methods, and hybrid techniques, which have emerged as advanced solutions to overcome the constraints of conventional IDS [90]. These models enhance detection accuracy, adaptability, and scalability, particularly in environments with encrypted traffic where traditional inspection methods are

ineffective. The representation highlights the ongoing shift from static, rule-dependent mechanisms to intelligent IDS architectures that can handle modern cybersecurity challenges [91].

2.4 Hybrid NIDS + HIDS Architectures

A recent and promising trend in Intrusion Detection System (IDS) research is the adoption of hybrid frameworks that combine both Network-based IDS (NIDS) and Host-based IDS (HIDS) with Artificial Intelligence (AI)-driven models [92, 93]. The motivation behind such integration is rooted in the recognition that no single detection mechanism is sufficient to address the wide variety of modern cyber threats. While NIDS provides visibility at the network layer by analyzing traffic flow patterns and metadata, HIDS monitors system-level activities, including system calls, log entries, and user behavior. Every approach has its own strengths and weaknesses: NIDS is effective for monitoring large-scale traffic but struggles in environments where encryption hides payloads. At the same time, HIDS provides detailed host-level insights but cannot capture coordinated attacks that spread across networks. By combining these two perspectives within a unified architecture, hybrid IDS frameworks can give a holistic defense mechanism that enhances both accuracy and coverage [94, 95].

$$B = \{B_1, B_2, \ldots, B_k, \ldots, B_l\} \quad \text{Eq (16)}$$

$$E_c = \frac{1}{K} \times \sum_{g=1}^{k} J_v^{b,t} - k_v \quad \text{Eq (17)}$$

$$B_{m,n}(q+1)\left(1 - \frac{1 - X(0,1) - X(-1,1)}{1 - c_{m,n} \times f_{mn}(q)}\right) = X(0,1) \times R_{s,n} \quad \text{Eq (18)}$$

One of the most prominent examples of such an approach is the Scale-Hybrid-IDS-Alert-Net (SHIA) framework. SHIA integrates distributed monitoring capabilities with deep learning algorithms to analyze massive volumes of network and host data in real time. Unlike traditional IDS that may focus only on traffic signatures or anomaly patterns, SHIA leverages a layered strategy where multiple data sources are fused to create a contextual understanding of potential threats. This makes the system not only scalable to enterprise-grade environments but also more resilient against adversaries who attempt to disguise their activities within encrypted or obfuscated traffic [96, 97].

In parallel, Natural Language Processing (NLP)-based methods have gained attention as part of hybrid IDS. By modeling system calls as sequences, similar to how words form sentences in

natural language, NLP-inspired IDS can detect subtle irregularities in host-level processes [98]. This is particularly useful for identifying stealthy intrusions that may not produce apparent anomalies in traffic flow but leave telltale signs in process execution patterns. Such techniques bridge the gap between traditional statistical IDS and modern AI-based approaches by introducing interpretability and sequence modeling into intrusion detection [99].

The strength of hybrid architectures lies not only in combining NIDS and HIDS, but also in integrating multiple analytical paradigms, such as machine learning, deep learning, and statistical analysis. For instance, while ML classifiers can quickly process structured traffic features, DL models like Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs) can capture hidden dependencies in encrypted traffic flows. When combined within a hybrid system, the complementary nature of these methods helps reduce false positives and improve the detection of both known and unknown threats [100].

Another advantage of hybrid systems is their adaptability to real-world deployment scenarios. Enterprises today often face multi-vector attacks where adversaries launch coordinated campaigns targeting both network infrastructure and host devices. A purely network-based or host-based IDS may miss critical stages of such attacks, but hybrid models can correlate evidence across different layers, thereby improving detection accuracy. Moreover, the distributed nature of frameworks like SHIA allows monitoring to scale across cloud environments, Internet of Things (IoT) ecosystems, and large organizational infrastructures.

Despite these benefits, challenges remain [101]. Hybrid IDS frameworks require significant computational power and storage resources, as they must process both traffic-level and host-level data simultaneously. Data synchronization across distributed monitoring points can also introduce complexity, and ensuring privacy compliance while collecting host-level data is another critical concern. Nevertheless, the trend toward hybrid architectures demonstrates a clear direction in IDS research: integration over isolation. Instead of relying on a single technique, modern IDS solutions are moving toward combining multiple perspectives, data sources, and analytical models to provide a comprehensive and adaptive defense against evolving cyber threats [102].

In summary, hybrid IDS architectures represent a significant advancement in the field of intrusion detection. By combining the strengths of NIDS and HIDS and leveraging advanced AI methods, such as deep learning and NLP, they provide a more robust defense against sophisticated intrusions, including those hidden within encrypted traffic. At the same time, challenges of scalability, resource usage, and privacy remain; hybrid frameworks like SHIA point to a future where IDS can operate effectively in real-world, large-scale, and highly dynamic environments [103].

2.7 Explainable AI (XAI) and Federated Learning in IDS

One of the main barriers to deploying AI-driven IDS in real-world environments is the lack of interpretability. Most Deep Learning (DL) models function as “black boxes,” making it difficult for analysts to understand why specific flows are flagged as malicious. Explainable AI (XAI) addresses this problem by providing transparency into model predictions. Techniques such as SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) enable security teams to trace alerts back to specific traffic features, enhancing trust and accountability in IDS operations [104].

Alongside interpretability, privacy concerns have become increasingly critical due to the widespread use of encrypted traffic. Federated Learning (FL) has emerged as a promising

solution, allowing IDS models to be collaboratively trained across multiple distributed datasets without requiring centralized data collection. Each participating node trains a local model and shares only parameter updates with a global server, which aggregates them to form an improved model. This not only preserves data privacy but also helps address dataset scarcity by leveraging diverse traffic sources across organizations.
Together, XAI and FL represent key enablers for the next generation of IDS—providing both transparency for human analysts and privacy-preserving scalability for distributed network environments [105].

2.8 Datasets Description and Pre-Processing in IDS

Datasets have always played a central role in the development, evaluation, and benchmarking of Intrusion Detection Systems (IDS). Since IDS models are heavily data-driven, the quality, diversity, and representativeness of the datasets used directly affect how well these models perform in detecting both known and unknown attacks. In the early stages of IDS research, benchmark datasets such as KDDCup99 and its improved version, NSL-KDD, served as the foundation for testing machine learning algorithms. These datasets included basic TCP/IP connection features and were widely used to compare different classifiers under standardized conditions. However, over time, they faced significant criticism. Researchers noted issues such as redundancy in records, outdated attack patterns, unrealistic traffic distributions, and the absence of encrypted flows. As a result, while they were helpful in academic experimentation, their applicability to real-world network environments was limited.

To overcome these shortcomings, more modern datasets were introduced. Among the most prominent are CICIDS2017 and UNSW-NB15, both of which include more realistic traffic scenarios and cover a broader range of attack types [16]. CICIDS2017, for instance, simulates real-world environments with both benign and malicious traffic, including attacks such as DoS, DDoS, botnets, and infiltration attempts. It also incorporates encrypted traffic flows, which are essential for evaluating IDS designed for modern networks. Similarly, UNSW-NB15 was developed to simulate enterprise-level traffic and contains a broader distribution of attack classes compared to earlier datasets. These improvements have made them popular benchmarks in current IDS research.

Despite these advances, limitations remain. Both CICIDS2017 and UNSW-NB15 suffer from issues such as class imbalance, where specific attack categories are underrepresented, leading to biased learning in machine learning and deep learning models. Additionally, while they are more representative than older datasets, they still fall short of replicating the scale, diversity, and dynamism of real-world enterprise traffic. High-speed, large-scale, and continuously evolving network environments introduce complexities that static benchmark datasets cannot fully capture. This gap has motivated researchers to explore alternative approaches, including the generation of synthetic datasets using Generative Adversarial Networks (GANs), federated learning with distributed data sources, and collaborative data-sharing initiatives to build more comprehensive benchmarks for IDS development. Table 5 provides an overview of some of the most commonly used datasets in IDS research, highlighting their core features, strengths, and limitations. Early datasets, such as KDDCup99 and NSL-KDD, were instrumental in benchmarking machine learning algorithms; however, their outdated attack patterns and lack of encrypted flows limit their applicability to modern environments. In contrast, more recent

datasets, such as CICIDS2017 and UNSW-NB15, attempt to simulate real-world traffic, including DoS, DDoS, botnet, and infiltration attacks. CICIDS2017 is notable for incorporating encrypted flows, while UNSW-NB15 offers broader attack diversity for enterprise-level scenarios. However, both suffer from challenges such as class imbalance and limited scalability, underscoring the need for datasets that more accurately reflect the large-scale and dynamic nature of modern networks.

Table 5. Commonly Used IDS Datasets and Their Limitations

Dataset	Features	Strengths	Limitations	Ref
KDDCup99	Basic TCP/IP features, connection logs	Benchmark for early IDS studies	Redundant, outdated, unrealistic	[106]
NSL-KDD	Cleaned version of KDDCup99	Reduced redundancy, easier benchmarking	Still outdated, lacks encryption	[107]
CICIDS2017	Modern traffic, botnets, DoS, DDoS	Includes encrypted flows, realistic mix	Imbalanced, limited scalability	[108]
UNSW-NB15	Simulated enterprise traffic with attacks	Broader attack diversity	Does not fully capture real-world dynamics	[109]
ADFA-LD	Linux system call logs	Useful for host-level intrusion detection	Limited to the Linux environment	[110]
TON_IoT	IoT and SCADA traffic	Realistic, multi-source data for IoT	Still under early adoption	[111]
Bot-IoT	IoT botnet attacks	Covers DDoS, DoS, keylogging, and infiltration	Does not include all IoT threats	[112]

From [110-112] presents datasets developed to address emerging domains such as host-level intrusion detection and IoT/SCADA environments. ADFA-LD focuses on Linux system call logs, making it valuable for host-based IDS research, though it remains limited to a specific operating system. TON_IoT introduces realistic, multi-source IoT and SCADA traffic, providing a much-needed benchmark for IoT security research. However, it is still in its early stages of adoption within the research community. Similarly, Bot-IoT captures a range of IoT-specific attack scenarios, including DDoS, DoS, keylogging, and infiltration; however, it does not comprehensively cover the full spectrum of IoT threats. Together, these datasets extend the scope of IDS evaluation beyond traditional enterprise networks, addressing the growing need for benchmarks that reflect the complexity of IoT and cyber-physical systems.

To provide a consolidated view of recent developments in Intrusion Detection Systems (IDS), this section compares key research studies across different approaches, datasets, and performance outcomes. The comparative table highlights how traditional machine learning models, deep learning architectures, and hybrid frameworks have evolved to address the challenges posed by encrypted traffic, scalability, and explainability. It also reflects the growing role of modern datasets such as CICIDS2017 and UNSW-NB15, alongside advanced techniques like Transformers, Explainable AI (XAI), and Federated Learning. Table 7 presents a comparative analysis of selected studies in IDS research, highlighting datasets, methods, performance metrics, and unique contributions.

Table 5. Commonly Used IDS Models

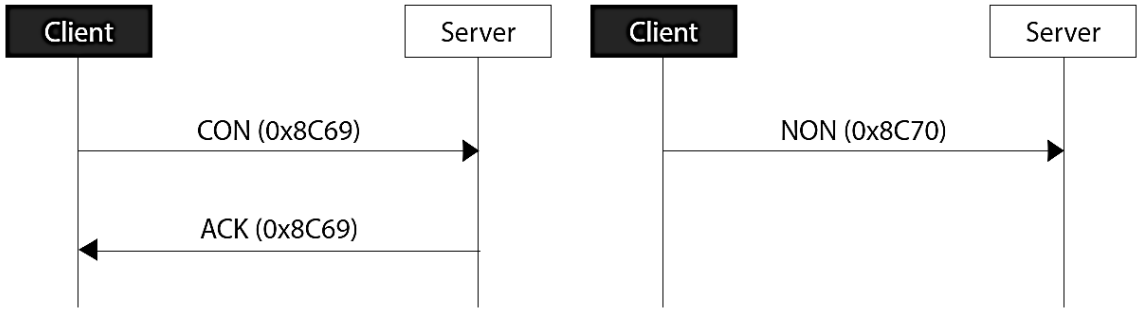
Datasets Used	Model	Key Metrics	Main Contribution	Ref
Botnet traffic dataset	ML-based classification (SVM, RF)	Accuracy ~85%	Applied ML techniques for botnet traffic detection; highlighted early ML limitations.	[113]
Benchmark datasets (general)	Deep Learning (CNN, RNN)	Accuracy ~88%	Provided foundational deep learning concepts that later influenced IDS applications.	[114]
Real-time network traces	Bro IDS system	High detection accuracy in real-time	Introduced Bro, an early real-time IDS, laying the foundation for traffic-based intrusion detection.	[115]
System call traces	Sequence-based IDS	Detected anomalies in call sequences	Demonstrated system call sequence analysis for anomaly detection.	[116]
Unix process traces	Self/non-self IDS	Detected deviations in process behavior	Proposed the "self/non-self" model, pioneering anomaly detection in host processes.	[117]
System call datasets	Pairgram-based anomaly detection	Improved detection precision	Modeled the frequency of lookahead pairs in system calls to enhance anomaly detection.	[118]

2.10 Research Gap Identification

The existing body of research on Intrusion Detection Systems (IDS) demonstrates significant progress, moving from signature-based detection toward machine learning, deep learning, and hybrid AI-driven frameworks. Comparative analyses reveal that advanced models, such as CNNs, RNNs, LSTMs, and Transformers, outperform traditional algorithms. Meanwhile, hybrid NIDS–HIDS solutions offer broader visibility across host and network environments. Likewise, Explainable AI (XAI) and Federated Learning have been introduced to address transparency and privacy issues. Despite these developments, several critical gaps remain unaddressed.

First, most IDS models continue to rely on limited or outdated datasets such as KDDCup99 and NSL-KDD, which fail to capture the scale, diversity, and encrypted nature of modern network traffic. Even more recent datasets, such as CICIDS2017 and UNSW-NB15, suffer from class imbalance and lack coverage of complex enterprise or IoT environments, raising concerns about the generalizability of trained models. This highlights a pressing need for large-scale, realistic, and continually updated datasets that accurately reflect real-world network dynamics.

Second, the increasing dominance of encryption has led to a loss of payload visibility for intrusion detection systems. Traditional deep packet inspection (DPI) techniques are now ineffective, forcing researchers to rely on metadata and traffic flow features. While promising, these indirect indicators are often insufficient to detect sophisticated or stealthy attacks. Thus, the challenge of designing an IDS capable of identifying intrusions in fully encrypted environments without violating privacy remains largely unresolved.



(a) Confirmable Message (b) Non-confirmable Message

FIGURE 4: Confirmable Messages Based On Ids (B) Non-Confirmable Messages Without Ids [119]

Although deep learning architectures achieve high accuracy, they remain computationally intensive and often unsuitable for real-time deployment in large enterprises or IoT networks. Scalability and efficiency issues hinder their adoption in practice, especially where lightweight solutions are required. Moreover, the "black-box" nature of deep models continues to restrict their usability, as security analysts demand explainable outputs to validate alerts and respond effectively [120]. IDS models still struggle with false positives, particularly in anomaly-based and deep learning approaches. Excessive false alarms not only overwhelm analysts but also reduce trust in the system, creating operational bottlenecks. Reducing false positives without compromising detection accuracy remains an open challenge in IDS research [121].

Finally, while hybrid architectures and federated approaches show promise, there is still limited research on integrating these methods into practical, resource-constrained, and privacy-sensitive environments. Existing frameworks often remain at the proof-of-concept stage, with little evidence of performance in real-time, enterprise-scale deployments [122].

2.11 Challenges and Research Directions

Despite significant progress in Machine Learning (ML) and Deep Learning (DL)-based Intrusion Detection Systems (IDS), several challenges continue to limit their practical deployment in real-world environments. While AI-driven IDS has demonstrated superior performance related to traditional signature-based or anomaly-based approaches, issues related to false positives, dataset quality, scalability, and explainability remain significant obstacles. Addressing these challenges is critical for moving from controlled experimental setups to operational, enterprise-level adoption [123].

A major ongoing challenge in IDS research is the large number of false positives. Anomaly-based and deep learning models, while effective at finding zero-day attacks, often misclassify benign activities as malicious. This generates a flood of unnecessary alerts, overwhelming security analysts and reducing system reliability. High false positive rates not only increase operational costs but also contribute to "alert fatigue," where critical threats may be ignored due to the excessive volume of alerts. Reducing false positives without sacrificing detection accuracy is therefore one of the key goals in IDS research [124].

Another major challenge is the scarcity of large-scale, varied, and encrypted traffic datasets. Many existing datasets, such as NSL-KDD, CICIDS2017, and UNSW-NB15, provide valuable

benchmarks, but they remain limited in scope. They usually fail to capture the diversity of real-world enterprise environments and the complexity introduced by encrypted traffic. Furthermore, class imbalance within these datasets makes it difficult for models to learn rare attack types successfully [125]. If IDS models are not trained on realistic and current datasets, they may overfit to controlled lab environments and fail to perform effectively in real-world deployments. This highlights the need for new strategies such as synthetic dataset generation using Generative Adversarial Networks (GANs) and collaborative data-sharing frameworks that preserve privacy while enabling broader access to representative traffic data [126].

Scalability is another pressing concern. Deep learning models, particularly architectures such as CNNs, LSTMs, and Transformers, require substantial computational resources. Training these models on large datasets demands high-performance GPUs or distributed computing clusters, which are not always available to organizations. Moreover, real-time intrusion detection in enterprise or cloud environments involves processing terabytes of network traffic per day, a scale that many current AI-based IDS cannot handle efficiently [127]. Developing lightweight models, optimizing architectures for real-time detection, and exploring distributed or parallelized deep learning frameworks are active areas of research aimed at overcoming scalability limitations.
A further barrier to adoption is the limitation in providing clarity in deep learning-based IDS. Most models act as "black boxes," making predictions without offering insight into their decision-making processes. For security analysts, it is critical to understand why a system flagged a particular activity as malicious, both to validate alerts and to take appropriate countermeasures. Without transparency, trust in AI-driven IDS remains limited. To overcome this challenge, researchers have developed Explainable AI (XAI) techniques, such as Shapley Additive explanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME), which provide post-hoc explanations of model predictions. These methods enable analysts to trace detected anomalies back to the specific features or patterns that influenced the model, thereby enhancing both usability and trust [128].

To overcome these challenges, several research directions have been proposed. Federated learning allows IDS models to be trained across multiple distributed systems without centralizing sensitive data, improving generalization while preserving privacy. Similarly, transfer learning enables models to adapt to new attack types or environments with minimal retraining, thereby reducing their dependency on large labeled datasets [129]. Hybrid frameworks, combining NIDS and HIDS with advanced DL models, have also shown promise in reducing false positives and improving detection accuracy in encrypted environments. Furthermore, research into resource-efficient AI models, such as pruning, quantization, and lightweight architectures, is opening possibilities for real-time IDS deployment in constrained environments like IoT networks [130].

Table 6. IDS Challenges and Emerging Research Models

Challenge	Limitation	Proposed Solution	Ref
High False Positives	Too many alerts	Context-aware DL, ensemble learning	[131]
Dataset Scarcity	Limited encrypted data	Synthetic dataset generation, federated learning	[132]
Scalability	Heavy computation needed	Distributed and parallel	[133]

		frameworks	
Lack of Explainability	Black-box models	XAI methods such as SHAP, LIME	[134]

In summary, while AI-driven IDS has advanced the state of cybersecurity, critical challenges remain, including false positives, dataset limitations, scalability issues, and concerns regarding interpretability. The combination of federated learning, transfer learning, XAI, and hybrid detection frameworks offers promising solutions to these problems. Continued research in these directions will pave the way for the development of an efficient, transparent, and scalable IDS capable of operating in modern encrypted environments. Above Table 8 summarizes key challenges in AI-driven IDS and their emerging solutions. High false positives are being mitigated through context-aware deep learning and ensemble methods, while dataset scarcity is addressed by synthetic data generation and federated learning. Scalability issues caused by heavy computation are being tackled with distributed and parallel frameworks. Finally, the limitation in providing clarity in deep learning models is countered by Explainable AI (XAI) techniques such as SHAP and LIME. These solutions underscore ongoing efforts to enhance the accuracy, scalability, and trustworthiness of IDS in real-world environments.

3. Proposed Deep Learning Approach for IDS

Deep Learning (DL) has emerged as one of the most powerful approaches for enhancing the performance of Intrusion Detection Systems (IDS), particularly in environments dominated by encrypted network traffic. Unlike traditional Machine Learning (ML) models that rely heavily on manual feature extraction, DL models are proficient in automatically learning complex, layered representations directly from raw or lightly preprocessed traffic data. This ability has enabled them to outperform earlier approaches in terms of accuracy, adaptability, and scalability, making them a compelling solution for modern cybersecurity challenges.

Convolutional Neural Networks (CNNs) have been widely applied in IDS due to their strength in detecting spatial dependencies and local patterns within traffic features. For example, CNNs can recognize anomalies in packet headers, flow statistics, or feature matrices by treating them as structured data representations similar to images. This capability enables CNN-based IDS to detect subtle patterns of malicious activity that shallow classifiers may overlook.

Recurrent Neural Networks (RNNs), along with their enhanced version, Long Short-Term Memory (LSTM) networks, are particularly effective for analyzing sequential and time-dependent data. Since network traffic often follows temporal dependencies, such as session-based activities or multi-stage attacks, these models are well-suited for identifying anomalies that unfold over time. LSTMs, in particular, overcome the vanishing gradient problem of standard RNNs, enabling them to capture long-range dependencies and patterns in traffic sequences.

More advanced architectures, such as Transformers and attention-based models, have recently been explored in IDS research. These models utilize self-attention techniques to capture background relationships across long sequences, thereby eliminating the need for recurrence and achieving the highest level of performance in handling large and complex network flows.

In addition, unsupervised DL techniques like autoencoders and Generative Adversarial Networks (GANs) have been applied for anomaly detection. Autoencoders learn compact latent representations of regular traffic and flag deviations as potential intrusions, while GANs generate

synthetic traffic data that helps train robust models and improve generalization. However, the effectiveness of these approaches often depends on the availability of large, high-quality datasets and significant computational resources, which remain a challenge for real-world deployment.

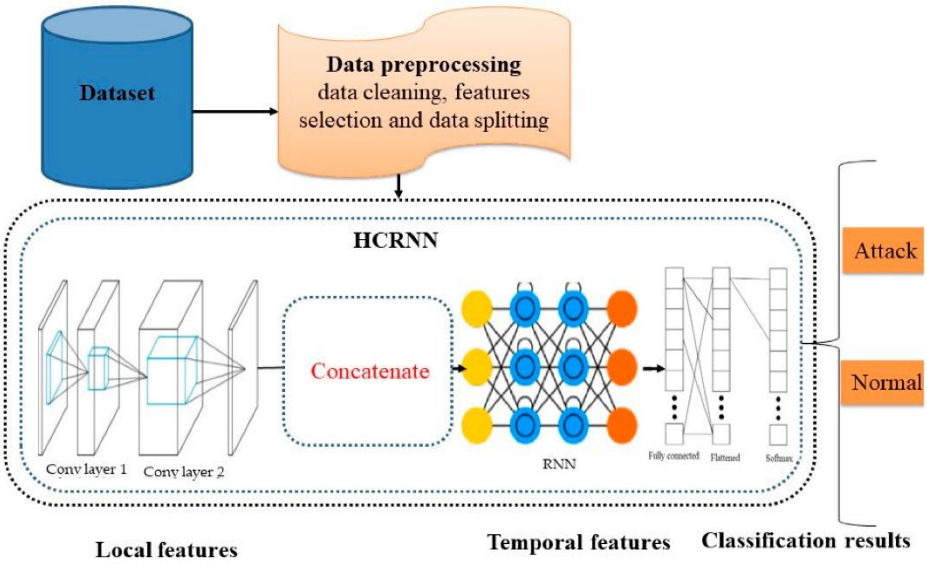


Figure 5. Proposed CNN and RNN based Encrypted Traffic IDS

Figure 4 illustrates the integration of Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) in an IDS framework designed for encrypted traffic analysis. The dataset undergoes data preparation steps, including cleaning, feature selection, and data splitting, before being passed into the hybrid CNN-RNN (HCRNN) model. CNN layers are responsible for extracting local spatial features, while RNN layers capture temporal dependencies within traffic sequences. These features are concatenated and processed through fully connected layers to generate classification outputs, distinguished between regular and attack traffic. This approach highlights the complementary strengths of CNNs and RNNs in handling both spatial and sequential aspects of encrypted network flows, thereby improving detection accuracy. The emergence of Transformer architectures has opened new possibilities for Intrusion Detection Systems (IDS), particularly in environments where encrypted traffic limits the effectiveness of conventional approaches. Unlike recurrent models such as RNNs and LSTMs, Transformers utilize self-attention mechanisms to capture global dependencies across entire sequences of traffic without relying on recurrence. This allows them to efficiently process large-scale network data while modeling long-range contextual relationships between packets.

In IDS research, Transformer-based models have shown strong potential in identifying complex, multi-stage cyberattacks that unfold across extended time windows. By attending to different parts of the input sequence, these models can detect subtle correlations between traffic flows that shallow classifiers might otherwise overlook. Recent studies have demonstrated that attention mechanisms not only improve detection accuracy in encrypted environments but also reduce the reliance on manual feature engineering, as the models can automatically learn hierarchical traffic representations.

Despite their strengths, Transformer models present challenges in terms of scalability and interpretability. Training such models requires large, high-quality datasets and powerful computational resources, which may not be readily available in many enterprise settings.

Moreover, the "black-box" nature of attention-based systems makes it difficult for analysts to understand why a particular flow was classified as malicious fully. Nevertheless, Transformers represent one of the most promising directions for IDS research, offering adaptability, scalability, and robustness in detecting sophisticated threats in encrypted networks.

The Proposed Technique works on the basis of below Algorithm:

Algorithm 1: Framework for Proposed IDS learning

Step 1. Initialize the training models $\{k_1, k_2, ...k_m\}$, learning rate 'η', regularization 'λ', model parameters ΘA, ΘB, datasets $\{L_1, L_2, ...L_m\}$, space feature M_a and M_b;

Step 2. Minimize *k(i)* parameter '*w*' is

$$Min_w^k(i) = \sum_{j=1}^{M} k_i(w \mid L_i)$$

Step 3. The objective of the training is

$$Min \sum_i [\| \theta_A M_i^A + \theta_B M_i^B] - [N_i \| + \frac{\lambda}{2}(\|\theta_A\|^2 + \|\theta_B\|^2)]$$

Step 4. The encrypted loss is

$$L = \left[\left[\sum_i ((U_i^A + U_i^B - N_i))^2 + \frac{\lambda}{2}(\theta_A^2 + \theta_B^2) \right]\right]$$

Step 5. The gradients are

$$\left[\left[\frac{\delta L}{\delta \theta_A} \right]\right] = \sum_i d_i M_i^A + \lambda \theta_A \text{ , and}$$

$$\left[\left[\frac{\delta L}{\delta \theta_B} \right]\right] = \sum_i d_i M_i^B + \lambda \theta_B$$

Step 6. The models are retrained

Step 7. Encrypts the data randomly

The proposed classifier contains i to represent random units of b-layer units and y to represent the total b-layer units.

$$S_i^{(b,t)} = \sum_{z=1}^{E} p_{iz}^{(b)} J_z^{(b-1,t)} + \sum_{i'}^{y} x_{ii'}^{(b)} J_{i'}^{(b,t-1)}$$

Eq (19)

$$J_i^{(b,t)} = \beta^{(b)}(S_i^{(b,t)})$$

Eq (20)

$$P(w) = \sqrt{\frac{t}{f(w)}} + \frac{t}{f(w)},$$

Eq (21)

$$f(w) = \frac{count_w}{totalno.oftokens},$$

Eq (22)

Figure 6 illustrates a proposed Intrusion Detection System (IDS) framework. In this setup, clients locally train models on their private datasets for several epochs and generate updates, without sharing raw data. These updates are then aggregated using the FedAvg algorithm to form a global model. The updated global parameters are redistributed to clients, enabling collaborative learning while preserving data privacy. This decentralized approach improves detection performance, reduces reliance on centralized data collection, and strengthens security against evolving threats.

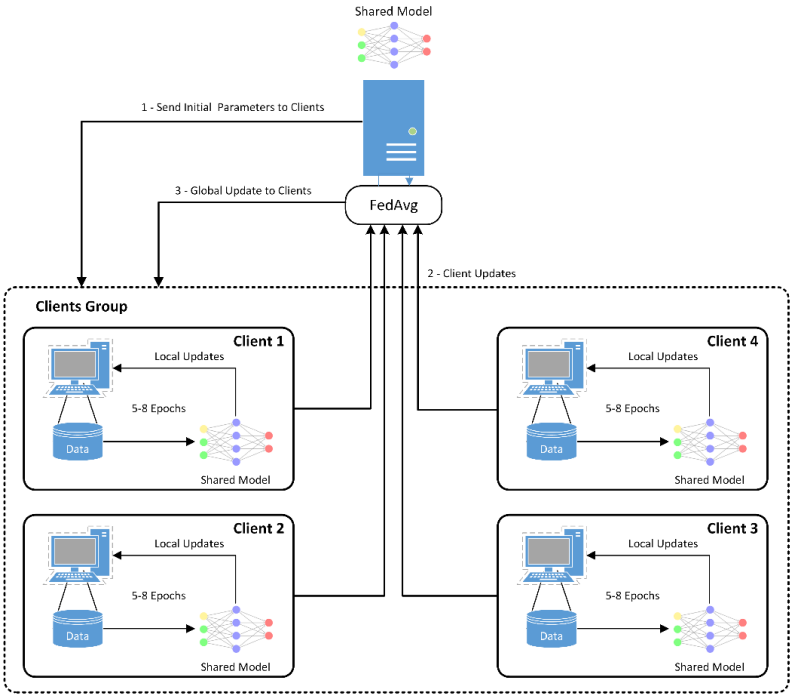


Figure 6. Proposed IDS Framework

The methodology is to ensure a comprehensive and unbiased synthesis of the existing research on Intrusion Detection Systems (IDS). The literature was collected from reputable academic databases, including IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Google Scholar, using a combination of keywords such as *Intrusion Detection System, AI-based IDS, Machine Learning IDS, Deep Learning IDS, Hybrid IDS, Encrypted Traffic IDS,* and *Explainable AI in IDS*. The primary focus was on studies published between 2010 and 2024, although earlier works were also considered to provide historical context and highlight the evolution of IDS approaches. To maintain relevance, studies were included if they proposed IDS techniques based on machine learning, deep learning, hybrid frameworks, federated learning, or explainable AI, and if they reported evaluation results using benchmark datasets such as NSL-KDD, CICIDS2017, UNSW-NB15, or other real-world traffic traces. Research that focused solely on traditional, rule-based IDS, without incorporating AI or lacking sufficient methodological and experimental detail, was excluded from the analysis.

$$\sum_{i=\{1,,,n\}/k}^{n} \frac{c_i}{\tau_i} + \frac{c_k + \alpha_k}{\tau_k} \qquad \text{Eq (23)}$$

While another task t_2 with intrusions arrive with the earliest deadline before the end of the execution task $t_1$then the length of the idle interval due to network delay and threat is denoted as λ_j and max time duration for the idle period is represented as α_j during longer data attack that can be measured using Eq. (10).

$$\sum_{i=\{1.,.,.n\}/(k,j)}^{n} \frac{c_i}{\tau_i} + \frac{c_k + \alpha_k}{\tau_k} + \frac{c_j + \alpha_j}{\tau_j} = 1 \qquad \text{Eq (24)}$$

Traditional to AI-based models, machine learning approaches, deep learning architectures such as CNNs, RNNs, LSTMs, and Transformers, hybrid NIDS–HIDS systems, and advanced techniques, including federated learning and explainable AI. In addition, a critical focus was placed on the role of datasets, particularly the strengths and weaknesses of commonly used benchmarks, as well as on how each study addressed challenges such as encryption, scalability, high false positive rates, and interpretability.

$$\sum_{i=\{1.,.,.n\}/(k,j)}^{n} \frac{c_0}{\tau_0} + \frac{c_0 + \alpha_0}{\tau_0} + \frac{c_0 + \alpha_0}{\tau_0} \qquad \text{Eq (25)}$$

$$\sum_{i=\{1.,.,.n\}/(k,j)}^{n} \frac{c_1}{\tau_1} + \frac{c_1 + \alpha_1}{\tau_1} + \frac{c_1 + \alpha_1}{\tau_1} \qquad \text{Eq (26)}$$

$$\sum_{i=\{1.,.,.n\}/(k,j)}^{n} \frac{c_3}{\tau_3} + \frac{c_3 + \alpha_3}{\tau_3} + \frac{c_3 + \alpha_3}{\tau_3} \qquad \text{Eq (27)}$$

$$\sum_{i=\{1.,.,.n\}/(k,j)}^{n} \frac{c_n}{\tau_n} + \frac{c_n + \alpha_n}{\tau_n} + \frac{c_n + \alpha_n}{\tau_n} \qquad \text{Eq (28)}$$

For comparison, performance metrics commonly reported in IDS research—such as accuracy, precision, recall, F1-score, and false positive rate—were used to evaluate the strengths and limitations of different approaches. By applying this methodology, the review ensures a structured and balanced examination of IDS research, highlighting not only technical advancements but also persistent gaps and challenges that must be addressed for future development.

4. Results and Discussion

The Intrusion Detection Systems (IDS), progressing from early static approaches to intelligent, adaptive solutions. Traditional systems relied heavily on rule-based and signature-driven techniques, which were highly effective in detecting well-documented attacks. However, these approaches soon proved insufficient in the face of rapidly evolving cyber threats. Various Malware, zero-day attacks, and advanced determined threats (APTs) demonstrated that systems based solely on predefined rules could not adapt to unknown attack behaviors. This shortcoming shifted research interest toward more flexible approaches, leading to the adoption of machine learning (ML) and later deep learning (DL) methods as the foundation of modern IDS design. This shift reflects a growing consensus in the research community: static mechanisms, while useful as a baseline, cannot provide adequate protection against modern, encrypted, and large-scale cyberattacks.

One of the most important insights gained from recent research is the dual role of encryption in cybersecurity. On one hand, encryption is vital for ensuring confidentiality, integrity, and trust in digital communication. Protocols such as TLS 1.3, QUIC, and VPN tunneling protect sensitive data from eavesdropping, thereby enhancing overall security. On the other hand, this very feature of encryption reduces network visibility, making it difficult for IDS to analyze payloads directly. Traditional tools such as deep packet inspection (DPI), once considered a cornerstone of network monitoring, are now largely ineffective in encrypted environments. To counter this challenge, researchers have turned to feature-based methods, relying on metadata such as packet size, flow duration, traffic timing, and inter-arrival intervals. [5], [9] While these approaches show significant promise, they simultaneously introduce additional challenges. Attackers are increasingly able to mimic standard traffic patterns, blending in with legitimate flows, which makes detection more challenging and raises the risk of false negatives.

Deep learning continues to play a central role in refining IDS accuracy. Convolutional Neural Networks (CNNs) have been proven to be valuable in analyzing spatial traffic features. At the same time, Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) models excel in capturing sequential and time-dependent traffic behavior. More advanced frameworks, such as Transformers and attention-based models, have been investigated for their ability to identify contextual relationships within traffic streams, offering strong detection capabilities even in highly dynamic environments. In addition, generative models like autoencoders and Generative Adversarial Networks (GANs) have been applied to anomaly detection, where they model normal behavior and flag deviations that suggest malicious activity. These methods often outperform traditional ML models in controlled experiments, particularly in terms of accuracy. However, their deployment in real-world environments continues to face significant obstacles, including computational overhead, lack of interpretability, and high false-positive rates. The trade-off between accuracy and operational feasibility remains a substantial barrier to large-scale adoption.

Another vital area of discussion is the role of hybrid IDS architectures. Combining network-based IDS (NIDS) with host-based IDS (HIDS) has been shown to create a more holistic defense framework. Such systems integrate both traffic-level metadata and host-level behavioral features, providing a richer context for detection. The Scale-Hybrid-IDS-Alert-Net (SHIA) is a notable example, demonstrating how distributed monitoring combined with deep learning can enhance real-time intrusion detection. However, hybrid systems also inherit challenges from both NIDS and HIDS, including scalability concerns, high resource demands, and reliance on limited benchmark datasets. Many proposed models perform well on public datasets but struggle to simplify successfully when deployed in real-world enterprise environments. This lack of robustness highlights the need for models trained on diverse and realistic datasets that capture the complexity of modern encrypted traffic.

Datasets represent a persistent bottleneck in IDS research. While benchmark datasets such as CICIDS2017 and UNSW-NB15 have advanced the field beyond earlier datasets like KDDCup99 and NSL-KDD, they still have limitations. CICIDS2017, for example, provides a valuable mix of modern attacks and encrypted flows but suffers from class imbalance issues and scalability

limitations. Similarly, UNSW-NB15 captures a wide range of attacks but fails to replicate the dynamic and heterogeneous nature of real-world traffic fully. The scarcity of large-scale, labeled, and encrypted datasets continues to limit the generalizability of models. Moreover, many datasets are collected in controlled lab environments, which means the resulting models often underperform when exposed to live network traffic with real-world noise, variations, and user behaviors. This limitation underscores the pressing need for collaborative data-sharing initiatives, federated learning frameworks, and the generation of synthetic datasets using generative models to supplement existing benchmarks.

The literature also emphasizes the growing importance of explainability and interpretability in IDS design. Analysts cannot blindly rely on detection outputs without understanding the reasoning behind them, especially in mission-critical environments like healthcare, finance, and defense. Explainable AI (XAI) has therefore been introduced as a promising way to address this gap. XAI tools such as SHAP and LIME make it possible to interpret predictions of complex models by highlighting which features contributed most to a detection decision. However, incorporating XAI into IDS introduces its own challenges: balancing transparency with computational efficiency, and ensuring that explanations remain actionable rather than overly technical. Without proper interpretability, even highly accurate IDS models risk rejection in practice due to a lack of trust among analysts.

The literature also highlights scalability as an issue. Since enterprise networks generate vast volumes of traffic, IDS is required to analyze data in real-time while avoiding performance bottlenecks. Many DL-based IDSs, while accurate, are resource-intensive and struggle to operate efficiently in high-speed environments. Distributed and parallel deep learning frameworks have been proposed as potential solutions; however, their practical implementation at scale remains in the early stages of research. Similarly, federated learning and transfer learning offer new pathways for developing IDS models that can adapt to new attacks while reducing dependence on centralized datasets. These methods are vital for environments where sensitive data cannot be shared due to privacy regulations.

4.1 Datasets Description and Pre-Processing in IDS

Datasets have always played a central role in the development, evaluation, and benchmarking of Intrusion Detection Systems (IDS). Since IDS models are heavily data-driven, the quality, diversity, and representativeness of the datasets used directly affect how well these models perform in detecting both known and unknown attacks. In the early stages of IDS research, benchmark datasets such as KDDCup99 and its improved version, NSL-KDD, served as the foundation for testing machine learning algorithms. These datasets included basic TCP/IP connection features and were widely used to compare different classifiers under standardized conditions. However, over time, they faced significant criticism. Researchers noted issues such as redundancy in records, outdated attack patterns, unrealistic traffic distributions, and the absence of encrypted flows. As a result, while they were helpful in academic experimentation, their applicability to real-world network environments was limited.

To overcome these shortcomings, more modern datasets were introduced. Among the most prominent are CICIDS2017 and UNSW-NB15, both of which include more realistic traffic scenarios and cover a broader range of attack types. CICIDS2017, for instance, simulates real-

world environments with both benign and malicious traffic, including attacks such as DoS, DDoS, botnets, and infiltration attempts. It also incorporates encrypted traffic flows, which are essential for evaluating IDS designed for modern networks. Similarly, UNSW-NB15 was developed to simulate enterprise-level traffic and contains a broader distribution of attack classes compared to earlier datasets. These improvements have made them popular benchmarks in current IDS research.

TABLE 7: Comparative Analysis Proposed Model Using Multiple Classifiers based on CICIDS2017

Classifier	Congestion Delay Time	IDs- A1	IDs- A2	IDs- A2	IDs- A3	IDs- A4	IDs- A5
RNN	0.011	57.34	54.32	62.19	62.19	3158	57.78	90.18
DT	0.041	62.19	52.34	57.34	39.65	3021	62.19	62.19
NBB	0.121	57.34	54.32	57.78	62.19	3158	57.78	57.34
RF	0.034	57.34	54.32	57.34	62.19	52.34	57.34	62.19
CNN	0.025	62.19	3158	57.78	57.34	54.32	57.78	57.34
ANN	0.018	39.65	3021	62.19	90.18	53.37	62.19	90.18

Despite these advances, limitations remain. CICIDS2017 suffer from issues such as class imbalance, where specific attack categories are underrepresented, leading to biased learning in machine learning and deep learning models. Additionally, while they are more representative than older datasets, they still fall short of replicating the scale, diversity, and dynamism of real-world enterprise traffic. High-speed, large-scale, and continuously evolving network environments introduce complexities that static benchmark datasets cannot fully capture. This gap has motivated researchers to explore alternative approaches, including the generation of synthetic datasets using Generative Adversarial Networks (GANs), federated learning with distributed data sources, and collaborative data-sharing initiatives to build more comprehensive benchmarks for IDS development. Table 5 provides an overview of some of the most commonly used datasets in IDS research, highlighting their core features, strengths, and limitations. Early datasets, such as KDDCup99 and NSL-KDD, were instrumental in benchmarking machine learning algorithms; however, their outdated attack patterns and lack of encrypted flows limit their applicability to modern environments. In contrast, more recent datasets, such as CICIDS2017 and UNSW-NB15, attempt to simulate real-world traffic, including DoS, DDoS, botnet, and infiltration attacks. CICIDS2017 is notable for incorporating encrypted flows, while UNSW-NB15 offers broader attack diversity for enterprise-level scenarios. However, both suffer from challenges such as class imbalance and limited scalability, underscoring the need for datasets that more accurately reflect the large-scale and dynamic nature of modern networks.

5. Conclusion

The rising sophistication of cyber threats, coupled with the near-universal adoption of encrypted communication protocols, has fundamentally altered the landscape of intrusion detection. Traditional Intrusion Detection Systems (IDSs), which once relied on techniques such as signature-based detection, anomaly-based detection, and stateful protocol analysis, now face significant limitations in addressing modern adversarial tactics. These classical methods were effective in environments where traffic was largely unencrypted and attack patterns were relatively well understood. However, they struggle to identify zero-day attacks, adapt to large-scale network traffic, or analyze encrypted payloads. This shortfall has created an urgent need for more advanced and intelligent solutions that can operate effectively under these challenging conditions. Artificial Intelligence (AI) has appeared as a capable answer to this need. Machine Learning (ML) and Deep Learning (DL) approaches have demonstrated the ability to surpass static, rule-based systems by learning from patterns and behaviors, rather than relying exclusively on known attack signatures. Among these, models like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) architectures, and Transformer-based models have demonstrated particular strength in capturing the complex spatial, temporal, and contextual dependencies inherent in modern network flows. These methods not only enhance accuracy but also allow for adaptive learning as new types of threats emerge. At the same time, the evolution of hybrid IDS frameworks has shown considerable potential. By combining the advantages of Network-based IDS (NIDS) and Host-based IDS (HIDS), these systems leverage both the wide visibility of network-level monitoring and the detailed granularity of host-level analysis. This integration enables more comprehensive detection, as demonstrated in frameworks such as SHIA, which strike a balance between scalability and distributed monitoring. Hybrid systems represent a significant step forward because they are not limited to a single perspective but instead provide a layered defense strategy that strengthens resilience against sophisticated adversaries.

Equally important is the creation of large-scale, encrypted traffic datasets that are realistic, diverse, and up-to-date. Such datasets should represent different types of networks, including enterprise, IoT, and industrial control systems, and should include encrypted traffic generated under real-world conditions. Collaborative data-sharing initiatives among industry, research institutions, and governments will be essential to making this vision a reality. Without such datasets, progress in IDS research will continue to be constrained by outdated benchmarks that do not reflect today's threat environment.

FUNDING STATEMENT: The authors received no specific funding for this study.

CONFLICTS OF INTEREST: The authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] Zhang, J.; Hua, Y.; Wang, H.; Song, T.; Xue, Z.; Ma, R.; Guan, H. Fedala: Adaptive local aggregation for personalized federated learning. In Proceedings of the AAAI Conference on Artificial Intelligence, Washington, DC, USA, 7–14 February 2023; pp. 11237–11244.

[2] Luo, J.; Wu, S. Adapt to adaptation: Learning personalization for cross-silo federated learning. In Proceedings of the IJCAI: Proceedings of the Conference, Vienna, Austria, 23–29 July 2022; Morgan Kaufmann: Amsterdam, The Netherlands; p. 2166.

[3] Tatipatri, N.; Arun, S. A Comprehensive Review on Cyber-attacks in Power Systems:

Impact Analysis, Detection and Cyber security. IEEE Access 2024, 12, 18147–18167.
[4] Singh, A.; Abosaq, H.A.; Arif, S.; Mushtaq, Z.; Irfan, M.; Abbas, G.; Ali, A.; Al Mazroa, A. Securing Cloud-Encrypted Data: Detecting Ransomware-as-a-Service (RaaS) Attacks through Deep Learning Ensemble. Comput. Mater. Contin. 2024, 79, 857–873.
[5] Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.
[6] P. Mathur, Overview of machine learning in healthcare, in: Machine Learning Applications using Python, A Press, Berkeley, CA, 2019, pp. 1–11.
[7] P. Guleria, M. Sood, Intelligent learning analytics in healthcare sector using machine learning, in: Machine Learning with Health Care Perspective, Springer, Cham, 2020, pp. 39–55.
[8] Gordon, T. & Kannel, W. B. Multiple risk functions for predicting coronary heart disease: The concept, accuracy, and application.Am. Heart J. 103, 1031–1039 (1982).
[9] Wilson, P. W. F. et al. Prediction of coronary heart disease using risk factor categories. Circulation 97, 1837–1847 (1998).
[10] Splunk Inc. State of Security 2024. 2024. Available online: https://www.splunk.com/en_us/form/state-of-security.html (accessed on 1 October 2024).
[11] Chapman, R. Ransomware Cases Increased by 73% in 2023 Showing Our Actions Have not Been Enough to Thwart the Threat. 2024. Available online: https://www.sans.org/blog/ransomware-cases-increased-greatly-in-2023/ (accessed on 3 October 2024).
[12] Li, W.; Jung, C.; Park, J. IoT Healthcare Communication System for IEEE 11073 PHD and IHE PCD-01 Integration Using CoAP. KSII Trans. Internet Inf. Syst. 2018, 12.
[13] service for low-power wide area networks: LO-CoAP-EAP. Sensors 2017, 17, 2646.
[14] Tamboli, M.B.; Dambawade, D. Secure and efficient CoAP based authentication and access control for Internet of Things (IoT). In Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics,
[15] Information Communication Technology (RTEICT), Bangalore, India, 20–21 May 2016; pp. 1245–1250.
[16] Krawiec, P.; Sosnowski, M.; Batalla, J.M.; Mavromoustakis, C.X.; Mastorakis, G. DASCo: Dynamic adaptive streaming over CoAP. Multimed. Tools Appl. 2018, 77, 4641–4660.
[17] Rahman, W.U.; Choi, Y.; Chung, K. Quality Adaptation Algorithm for Streaming over CoAP. In Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC),
[18] Guo, X., Aviles, G., Liu, Y., Tian, R., Unger, B. A., Lin, Y. H. T., & Kampmann, M. (2020). Mitochondrial stress is relayed to the cytosol by an OMA1–DELE1–HRI pathway. Nature, 579(7799), 427–432.
[19] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023
[20] Imtiaz, M. A., Amir, A., Bakhet, S., Siddique, H., & Rizwan, S. M. (2025). An

Optimal Diabetic Retinopathy Detection and Classification Approach based on integrated Hybrid Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(2).

[21] Ayub, N., Uzair, M., Din, I., Ali, A., Khan, H., Yuldashev, F., & Makhmudov, S. (2025). An Efficient Human Activity Recognition (HAR) Model Based on Convolutional Neural Networks for Computing Devices Aiming to Reduce Latency and Tackle the Inactivity of Gadgets. Engineering, Technology & Applied Science Research, 15(6), 28885-28890.

[22] Moustafa, N.; Koroniotis, N.; Keshk, M.; Zomaya, A.Y.; Tari, Z. Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions. IEEE Commun. Surv. Tutor. 2023, 25, 1775–1807.

[23] Alspach, K. Network Security Devices Are the Front Door to an IT Environment, But Are They Under Lock and Key? CRN Article. 2024. Available online: https://www.crn.com/news/security/2024/network-security-devices-are-the-front-door-to-an-it-environment-but-are-they-under-lock-and-key .

[24] Chen, Y.; Cui, M.; Wang, D.; Cao, Y.; Yang, P.; Jiang, B.; Lu, Z.; Liu, B. A survey of large language models for cyber threat detection. Comput. Secur. 2024, 145, 104016.

[25] Gupta, M.; Akiri, C.; Aryal, K.; Parker, E.; Praharaj, L. From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. IEEE Access 2023, 11, 80218–80245.

[26] Khan, H. M. S., Hayat, C. M. A., Tayyab, H., & Ali, K. (2024). An Enhanced Cost Effective and Scalable Network Architecture for Data Centers. Spectrum of Engineering Sciences, 2(4), 1-32.

[27] Rafay, A., Salman, W., Yahya, G., & Malik, U. (2024). SD Network based on Machine Learning: An Overview of Applications and Solutions. Spectrum of Engineering Sciences, 2(4), 150-165.

[28] Javed, M. A., Ahmad, M., Ahmed, J., Rizwan, S. M., & Tariq, A. (2025). An Enhanced Machine Learning based Data Privacy and Security Mitigation Technique: An Intelligent Federated Learning (FL) Model for Intrusion Detection and Classification System for Cyber-Physical Systems in Internet of Things (IoTs). Spectrum of Engineering Sciences, 3(2), 377-401.

[29] Aziz, R., Mehmood, A., Tariq, A., Nasim, F., Farooq, U., Naqvi, S. A. A., & Khan, H. (2025). Critical Evaluation of Data Privacy and Security Threats: An Intelligent Federated Learning-based Intrusion Detection System Poisoning Attack and Defense for Cyber-Physical Systems its Issues and Challenges Related to Privacy and Security in IoT. The Asian Bulletin of Big Data Management, 5(1), 73-84.

[30] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[31] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[32] Waleed, R., Ali, A., Tariq, S., Mustafa, G., Sarwar, H., Saif, S., ... & Uddin, I. (2024). An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based

MEAN Stack Technology Applications. Bulletin of Business and Economics (BBE), 13(2), 200-206.

[33] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[34] Mumtaz, J., Bakhet, S., Javed, A., Naz, A., Rashail, M., & Khan, H. (2025). An Intelligent Diagnosis and Tumor Segmentation Method based on MRI Images Using Pre-trained Deep Convolutional Neural Networks (CNNs). The Asian Bulletin of Big Data Management, 5(1), 147-163

[35] Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

[36] Noor, H., Khan, H., Din, I. U., Tariq, M. I., Amin, M. N., & Fatima, M. Virtual Memory Management Techniques. Securing the Digital Realm, 126-137.

[37] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[38] Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

[39] Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[40] FDM: Fuzzy-optimized Data Management Technique for Improving Big Data Analytics. IEEE Transactions on Fuzzy Systems, 29(1), 177–185. Manogaran, G., Shakeel, P. M., Priyan, R. V., Chilamkurti, N., & Srivastava, A. (2019). Ant colony optimization-induced route optimization for enhancing the driving range of electric vehicles. International Journal of Communication Systems, e3964. https://doi.org/10.1002/dac.3964

[41] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[42] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

[43] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[44] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by

unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[45] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[46] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[47] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[48] Sarker, I.H.; Khan, A.I.; Abushark, Y.B.; Alsolami, F. Internet of things (iot) security intelligence: A comprehensive overview, machine learning solutions and research directions. Mob. Netw. Appl. 2023, 28, 296–312.

[49] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[50] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[51] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[52] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

[53] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[54] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[55] Kumar, S.; Verma, P.K.; Verma, R.; Alsabaan, M.; Abdelkader, T. Internet of Things: Classification, Challenges, and Solutions. In Applications of Computational Intelligence Techniques in Communications, 1st ed.; CRC Press: Boca Raton, FL, USA, 2024; pp. 137–172.

[56] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[57] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A

Review. Spectrum of engineering sciences, 2(3), 420-454.

[58] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[59] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[60] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[61] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[62] Gordon, T. Diabetes, blood lipids, and the role of obesity in coronary heart disease risk for women. Ann. Intern. Med. 87, 393 (1977).

[63] Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

[64] Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533–536.

[65] Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

[66] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[67] Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

[68] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

[69] Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

[70] Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos, G.A.; Wang, Y.; Müller, C.A.; Lipps, C.; Júnior, R.T.S.; Vidal Filho, W.B.; et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

[71] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[72] Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

[73] Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

[74] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

[75] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, “An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[76] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[77] Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

[78] Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. Engineering, Technology & Applied Science Research, 15(2), 21279-21283.

[79] Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

[80] Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

[81] Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics, 126.

[82] Ayub, N., Iqbal, M. W., Saleem, M. U., Amin, M. N., Imran, O., & Khan, H. (2025). Efficient ML Technique for Brain Tumor Segmentation, and Detection, based on MRI Scans Using Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(3), 186-213.

[83] Saif, S., Hamayun Khan, A. A., Albouq, S., Hussain, M. Z., Hasan, M. Z., Uddin, I., ... & Husain, M. AN EFFICIENT MACHINE LEARNING-BASED DETECTION AND PREDICTION MECHANISM FOR CYBER THREATS USING INTELLIGENT FRAMEWORK IN IOTS. Vol.-15, No.-8, August (2024) pp 191-206

[84] Anas, M., Imtiaz, M. A., Saad Khan, A. A., Naghman, N. F., Khan, H., & Albouq,

S. AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING. Vol.-20, No.-3, March (2025) pp 54 - 72

[85] Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

[86] Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). Thermal-aware real-time task schedulabilty test for energy and power system optimization using homogeneous cache hierarchy of multi-core systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

[87] Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Impact of adopting robots as teachers: a review study. In 2022 International Conference on Emerging Technologies in Electronics, Computing and Communication (ICETECC) (pp. 1-9). IEEE.

[88] Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

[89] Ayub, N., Bakhet, S., Arshad, M. J., Saleem, M. U., Anam, R., & Fuzail, M. Z. (2025). AN ENHANCED MACHINE LEARNING AND BLOCKCHAIN-BASED FRAMEWORK FOR SECURE AND DECENTRALIZED ARTIFICIAL INTELLIGENCE APPLICATIONS IN 6G NETWORKS USING ARTIFICIAL NEURAL NETWORKS (ANNS). Spectrum of Engineering Sciences, 3(4), 348-364.

[90] Ghafoor, U., Ayub, N., Yaseen, A., Anas, M., Farooq, I., Khan, S., & Naghman, N. F. (2025). AI Assisted Heart Disease Prediction and Classification and Segmentation based on PIMA and UCI Machine Learning Datasets. Annual Methodological Archive Research Review, 3(7), 248-276.

[91] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[92] Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Blockchain-based Privacy Preservation Framework for IoT-Based Information Systems. In 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS) (pp. 1-7). IEEE, 2022

[93] Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

[94] Ali, M., Cheema, S. M., Aslam, Z., Naz, A., & Ayub, N. (2023, March). CBAI: Cloud-Based Agile Infrastructure for Enhancing Distributed Agile Development. In 2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE.

[95] Ayub, N., Yaseen, A., Amin, M. N., Rizwan, S. M., Farooq, I., & Hussain, M. Z. (2025). Reliable Federated Learning (Rdl) Assisted Intrusion Detection And Classifications Approach Using (Ssl/Tls) For Network Security. Annual Methodological

Archive Research Review, 3(7), 376-400.

[96] Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

[97] Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

[98] Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

[99] Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

[100] Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

[101] Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ... & Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-19067.

[102] Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.

[103] Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey. The Asian Bulletin of Big Data Management, 5(1), 1-14.

[104] Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

[105] Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

[106] Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on Convolutional Neural Network in Machine Learning Framework.

[107] Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

[108] Farooq, I., Ahmed, S. A., Ali, A., Warraich, M. A., Aqeel, M., & Khan, H. (2024). Enhanced Classification of Networks Encrypted Traffic: A Conceptual Analysis

of Security Assessments, Implementation, Trends and Future Directions. The Asian Bulletin of Big Data Management, 4(4), 500-522.

[109] Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

[110] Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

[111] Adil, M. U., Ali, S., Haider, A., Javed, M. A., & Khan, H. (2024). An Enhanced Analysis of Social Engineering in Cyber Security Research Challenges, Countermeasures: A Survey. The Asian Bulletin of Big Data Management, 4(4), 321-331.

[112] Maqsood, M., Dar, M. M., Javed, M. A., & Khan, H. (2024). A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective. The Asian Bulletin of Big Data Management, 4(4), 355-368.

[113] Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

[114] Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

[115] Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

[116] Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

[117] Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

[118] Farooq, M., Younas, R. M. F., Qureshi, J. N., Haider, A., & Nasim, F. (2025). Cyber security risks in DBMS: Strategies to mitigate data security threats: A systematic review. Spectrum of engineering sciences, 3(1), 268-290.

[119] Ayub, N., Habib, Z., Bakhet, S., Riaz, S., Rizwan, S. M., Abid, M., ... & Khan, H. (2025). An Optimal Ai & Deep Learning Mechanism For Mitigating Hacking Threat Identification Using Secure Network Infrastructure Based On Linux And Software-Defined Network (Sdn). Spectrum of Engineering Sciences, 3(5), 675-687.

[120] Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

[121] Ayub, N., Anwer, M. A., Iqbal, A., Rizwan, S. M., Shahbaz, A., Abid, M. H., & Rafi, S. (2025). Enhanced ML Framework based on Artificial Neural Network for countermeasures of Data Protection and Network Vulnerabilities Detection in Industrial Internet of Things. Annual Methodological Archive Research Review, 3(5), 410-431.

[122] Akhtar, M. H., Ali, A., Ali, S., Nasim, F., Aziz, M. H., Khan, H., & Naqvi, S. A. A. (2025). A Novel Machine Learning Approach for Database Exploitation to Enhance Database Security: A Survey. Spectrum of Engineering Sciences, 3(2), 26-57.

[123] Jabeen, T., Mehmood, Y., Khan, H., Nasim, M.F. and Naqvi, S.A.A., 2025. Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), pp.143-161.

[124] Jindal, A., Aujla, G. S., & Kumar, N. (2019). SURVIVOR: A blockchain-based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. Computer Networks, 153, 36–48. Khoramshahi, M., & Billard, A. (2019). A dynamical system approach to task adaptation in physical human-robot interaction. Autonomous Robots, 43(4), 927–946.

[125] Lin, K., Li, Y., Sun, J., Zhou, D., & Zhang, Q. (2020). Multi-sensor fusion for a body sensor network in a medical human-robot interaction scenario. Information Fusion, 57, 15–26. Manogaran, G., Baskar, S., Hsu, C. H., Kadry, S. N., Sundarasekar, R., Kumar, P. M., & Muthu, B. A. (2021).

[126] Ghabban, F.M.; Alfadli, I.M.; Ameerbakhsh, O.; AbuAli, A.N.; Al-Dhaqm, A.; Al-Khasawneh, M.A. Comparative analysis of network forensic tools and network forensics processes. In Proceedings of the 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Cameron Highlands, Malaysia, 15–17 June 2021; pp. 78–83. [Google Scholar]

[127] Breitinger, F.; Hilgert, J.N.; Hargreaves, C.; Sheppard, J.; Overdorf, R.; Scanlon, M. DFRWS EU 10-year review and future directions in Digital Forensic Research. Forensic Sci. Int. Digit. Investig. 2024, 48, 301685. [Google Scholar] [CrossRef]

[128] Nandita, G.; Munesh Chandra, T. Malicious host detection and classification in cloud forensics with DNN and SFLO approaches. Int. J. Syst. Assur. Eng. Manag. 2024, 15, 578–590.

[129] Pandey, B.; Pandey, P.; Kulmuratova, A.; Rzayeva, L. Efficient usage of web forensics, disk forensics, and email forensics in the successful investigation of cybercrime. Int. J. Inf. Technol. 2024, 16, 3815–3824.

[130] Alam, M.N.; Kabir, M.S. Forensics in the Internet of Things: Application Specific Investigation Model, Challenges and Future Directions. In Proceedings of the 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, 26–28 May 2023; pp. 1–6. [Google Scholar]

[131] Zhang, H. Simulation of network forensics model based on wireless sensor networks and inference technology. Meas. Sens. 2024, 34, 101261.

[132] Kamble, D.; Rathod, S.; Bhelande, M.; Shah, A.; Sapkal, P. Correlating forensic data for enhanced network crime investigations: Techniques for packet sniffing, network forensics, and attack detection. J. Auton. Intell. 2024, 7, 1272.

[133] Ferrag, M.A.; Ndhlovu, M.; Tihanyi, N.; Cordeiro, L.C.; Debbah, M.; Lestable, T.; Thandi, N.S. Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices. IEEE

Access 2024, 12, 23733–23750.

[134] Menard, P., & Bott, G. J. (2020). Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. Computers & Security, 95, 101856.