Explainable AI-Driven Zero Trust Anomaly Detection for Encrypted Traffic

Chalaka Perera
Department of Computer Engineering
University of Peradeniya
Sri Lanka
e20288@eng.pdn.ac.lk

Janith Wanasinghe
Department of Computer Engineering
University of Peradeniya
Sri Lanka
e20420@eng.pdn.ac.lk

Sandaru Wijewardhana
Department of Computer Engineering
University of Peradeniya
Sri Lanka
e20449@eng.pdn.ac.lk

Dr. Suneth Namal Karunarathna
Department of Computer Engineering
University of Peradeniya
Sri Lanka
namal@eng.pdn.ac.lk

Dr. Upul Jayasinghe
Department of Computer Engineering
University of Peradeniya
Sri Lanka
upuljm@eng.pdn.ac.lk

***Abstract*—The modern cybersecurity methods are more focused on encryption protocols to protect data privacy and MitM attacks but with those mechanisms traditional intrusion detection systems (IDS) are blinded. Additionally, the architectural method is shifting from perimeter-based models to Zero-Trust Architecture (ZTA) which demands the continuous, granular verification of every network entity. While Deep Learning (DL) models have demonstrated the capability to detect anomalies within encrypted streams without decryption, their opaque "black-box" nature creates a trust deficit that hinders their deployment in automated ZTA policy enforcement. This literature review provides a comprehensive critical analysis of peer-reviewed studies at the intersection of ZTA, Encrypted Traffic Analysis (ETA), and Explainable AI (XAI). It evaluates the efficacy of current flow-based feature extraction methods, compares the operational viability of XAI techniques like SHAP and LIME in real-time environments, and identifies a critical research gap the lack of unified frameworks that can detect, explain, and block malicious encrypted traffic with the speed required for modern high bandwidth networks.**

***Index Terms*—Zero-Trust Architecture (ZTA), Encrypted Traffic Analysis (ETA), Explainable AI (XAI), Network Anomaly Detection, Deep Learning, Automated Policy Enforcement.**

I. Introduction

A. Challenge in Encrypted Traffic Analysis

The digital landscape has changed significantly in terms of data transport security. Due to privacy concerns and regulations like GDPR, encryption has become the standard for network communication. Recent reviews, including the 2024 analysis by Ji et al. [1], show that most global web traffic is now encrypted using protocols like HTTPS and TLS. While this shift effectively reduces risks from eavesdropping and man-in-the-middle (MitM) attacks, it has inadvertently created a situation known as "going dark" for network defenders. Traditional security tools, especially Deep Packet Inspection (DPI), depend on analyzing the payload of data packets to identify malicious signatures. In an encrypted environment, these payloads are hidden, making DPI ineffective.

This lack of visibility has been exploited by threat actors. Adversaries now commonly use encrypted tunnels to hide malware distribution, command and control (C2) communications, and data exfiltration efforts. Research by Han et al. [2] shows that over 90% of malware threats now use encryption to bypass legacy firewalls. Similarly, Xing and Wu [3] find that standard anomaly detection methods fail with these invisible channels because they cannot differentiate between legitimate high entropy data (like video streaming) and malicious high entropy data (like ransomware encryption). Consequently, the modern cybersecurity challenge is not just about blocking known threats but identifying malicious intent concealed within seemingly legitimate, hidden data streams. This contrast between legacy clear-text inspection and modern encrypted "blind spots" is illustrated in Fig. 1.

B. The Zero-Trust Imperative

Alongside the rise of encryption is the decline of traditional perimeter-based security models. The loss of the corporate network boundary, driven by cloud computing, remote work, and the Internet of Things (IoT), has made the idea of "trusted internal networks" outdated. In response, organizations are moving towards Zero-Trust Architecture (ZTA).

ZTA is not just one technology, it is a strategic approach defined by the principle "never trust, always verify." As explained by Dhiman et al. [4] in their comparative study, ZTA requires that every access request be authenticated, authorized, and encrypted before access is granted. Importantly, this verification must be continuous, trust is diminishing and must be reassessed in real-time based on user behavior and context. Sarkar [5] adds that ZTA must extend beyond basic identity checks to evaluate the quality of the connection itself. However, implementing ZTA is fundamentally challenged by the lack of transparency in encrypted traffic. A Policy Enforcement Point (PEP) cannot effectively verify a connection if it cannot inspect traffic patterns for signs of compromise.

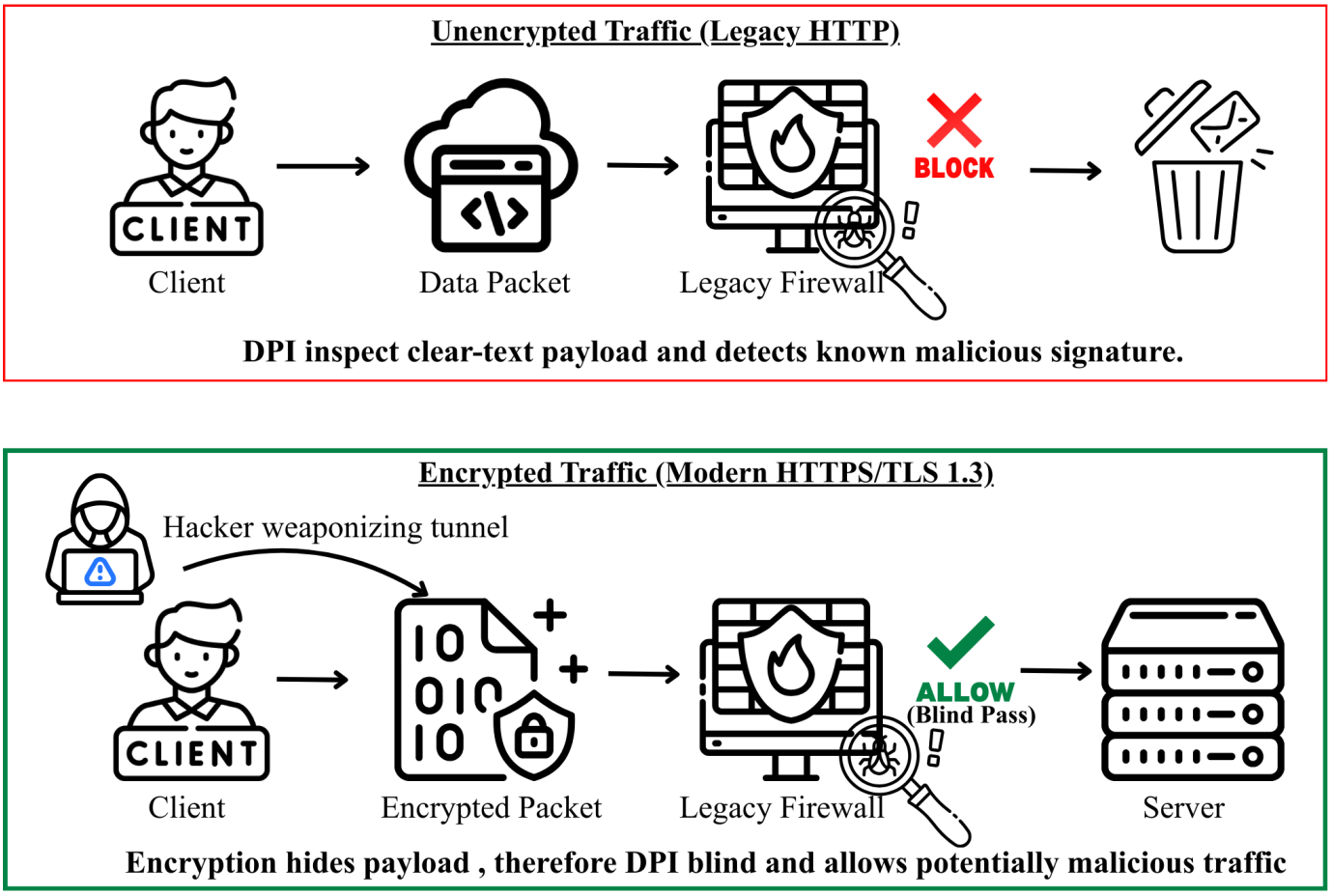

Fig. 1. Comparison between legacy unencrypted HTTP traffic, where Deep Packet Inspection (DPI) can inspect payloads and block known malicious signatures, and modern encrypted HTTPS/TLS traffic, where encryption hides payload contents and blinds traditional DPI-based firewalls.

C. The AI Transparency Gap

To address this issue, researchers are looking to Artificial Intelligence (AI) and Deep Learning (DL). As noted by Kodi [6], these models can identify malicious patterns in encrypted traffic by examining side channel features like packet timing, size, and direction without the need to decrypt the payload. Kim and Kim [7] show that Autoencoder-based models can detect anomalies in encrypted datasets and maintain high precision. Likewise, Liu and Wang [8] use Convolutional Neural Networks (CNNs) to analyze network flows as if they were images, achieving notable accuracy.

While these models achieve high detection rates, they create a new vulnerability known as the ”Black Box” problem. In a Zero Trust environment, security decisions can lead to immediate automated actions, such as isolating a device or revoking a user's credentials. If these decisions come from a non-transparent Neural Network that cannot articulate its reasoning, security teams face a difficult choice to trust the AI blindly and risk disruptions from false positives or ignore it and risk a security breach. Kalutharage et al. [9] describe this as a lack of ”semantic mapping” the AI knows something is wrong but cannot explain what. Nazat et al. [10] argue that this lack of transparency undermines the ”verify” principle of Zero Trust. Therefore, this review contends that integrating Explainable AI (XAI) is not just an enhancement but a necessity for operation.

II. The Paradigm Shift to Zero-Trust Architecture (ZTA)

A. Architectural Evolution and Cost-Benefit Analysis

Transitioning to Zero Trust signifies a complete rethink of network structure. Traditional models used Virtual Private Networks (VPNs) to tunnel traffic into a “trusted” zone. Adahman et al. [11] present a thorough cost effectiveness analysis of this transition. Their research challenges the notion that ZTA is overly expensive, showing that when the long-term costs of data breaches, ransomware recovery, and VPN management are considered, ZTA offers a better return on investment. They argue that VPNs have become single points of failure, while ZTA's distributed architecture reduces the impact of any single compromised credential. However, the operationalization of ZTA is more complex. Several studies, including those by

Micheal [12] and Kommera [13], break down the architecture into components such as the Policy Engine (PE) that decides access, the Policy Administrator (PA) that establishes the connection, and the Policy Enforcement Point (PEP) acting as the gatekeeper. The literature consistently points out that the effectiveness of this trio relies entirely on the quality of data fed into the Policy Engine. If the PE cannot see encrypted traffic patterns, the whole system fails to detect internal threats.

B. Zero-Trust in Dynamic Environments (Cloud & IoT)

Applying ZTA is further complicated by the dynamic nature of modern infrastructure. Guo et al. [14] explore ZTA in Software Defined Networking (SDN) and propose an "Intelligent Zero Trust" framework (IZTSDN). Their work indicates that static firewall rules do not align with temporary containers and serverless functions. In this context, "identity" is more than just a username. It is a complex mixture of workload IDs, API tokens, and behavioral patterns. The Internet of Medical Things (IoMT) introduces a unique challenge. As mentioned by Ogunmolu [15] and Gundaboina [16], healthcare settings need ZTA to protect sensitive patient data (in compliance with HIPAA) but cannot afford the latency or "false blocks" that might disrupt essential care devices. A ZTA system in a hospital must be "fail-open" or highly intelligent to differentiate between a hacker and a doctor accessing records during an emergency. Tabassum et al. [17] stress that in smart health systems, anomaly detection must be context-sensitive. A spike in data transmission could indicate either a firmware update or a data exfiltration attempt. Telling the difference without decrypting data requires thorough behavioral analysis.

C. Performance Overhead and Feasibility

A crucial but often overlooked element in the literature is the performance cost of ZTA. Rodigari et al. [18] perform a performance analysis of ZTA in multi cloud settings, specifically examining service meshes like Istio. Their findings are significant for this review, implementing the ongoing mutual TLS authentication and authorization checks required by ZTA introduces noticeable latency and CPU overhead. This creates a challenge for any proposed Anomaly Detection system. If an AI model takes several seconds to analyze a flow and produce an explanation, it causes a bottleneck that harms user experience, violating the usability standard for effective security. Therefore, the literature suggests that any AI-driven ZTA solution must be lightweight and fast, a challenge that conflicts with the trend of increasingly large Deep Learning models. The interaction between the Policy Engine, Policy Administrator, and Policy Enforcement Point in a Zero-Trust deployment, along with continuous monitoring, is summarized in the end-to-end workflow shown in Fig. 2.

III. Anomalies in the Dark: Encrypted Traffic Analysis (ETA)

A. From Deep Packet Inspection to Flow-Based Analysis

With Deep Packet Inspection (DPI) becoming outdated, researchers now focus more on "Flow-Based" analysis. In this method, network traffic is seen as a series of time-based events, not as readable text data. Yin et al. [19] show that this method works well by looking at the unencrypted headers (IP, TCP, UDP) that must stay visible for routing. They explain that even without reading the payload, the overall pattern or shape of the traffic—the metadata—is enough to identify certain malware families. For example, the sizes of the first few packets in a TLS handshake can reveal the cipher suite and client hello details, which can act like a fingerprint for specific attack tools. Long and Zhang [20] introduce a more detailed method using Parallel Stacked Autoencoders (SAE). Their system collects features from encrypted traffic by studying the statistical patterns of bytes. They say that even though encryption hides the payload, it does not hide the behavior of the application sending the traffic. For example, a video stream shows a bursty traffic pattern, while a file download is more continuous. Malware beacons usually send very short, regular bursts. By giving these patterns to a deep learning model, they achieved over 99% detection accuracy.

B. Deep Learning Approaches

- The increasing complexity of flow-based features has caused researchers to move from simple statistical models to Deep Learning methods.
- CNNs for Traffic Imaging: Liu and Wang [8] treat network traffic analysis like a computer vision task. They change flow data into 2D images (grayscale pictures that show packet sizes and timing) and then use Convolutional Neural Networks (CNNs) to classify them. Their results show that CNNs are very good at finding small spatial patterns in traffic that simpler, linear models cannot detect.
- Handling Imbalanced Data: A common problem in research is the "needle in a haystack" situation: in real networks, 99.9% of traffic is normal, and only a tiny amount is malicious. Kim and Kim [7] address this by creating feature extraction methods that work well even when the data is highly imbalanced. They use an Autoencoder that is trained only on normal traffic. When the model sees attack traffic, the reconstruction error becomes high, which signals an anomaly. This unsupervised method is important for finding zero-day attacks, which do not have any known signature.
- Hybrid Models: Bakhshi and Ghita [21] suggest a hybrid deep learning approach that mixes different neural network types to improve accuracy and reliability. But they also highlight a major limitation: using only statistical features can cause many false positives, especially when the model sees unusual but harmless traffic, such as high-bandwidth video streaming or large file downloads.

C. Limitations of Current ETA Methods

Despite these successes, significant limitations remain. Edozie et al. [22] review the advances in AI for telecom networks and note that while models like Generative Adversarial Networks (GANs) show promise, they are computationally

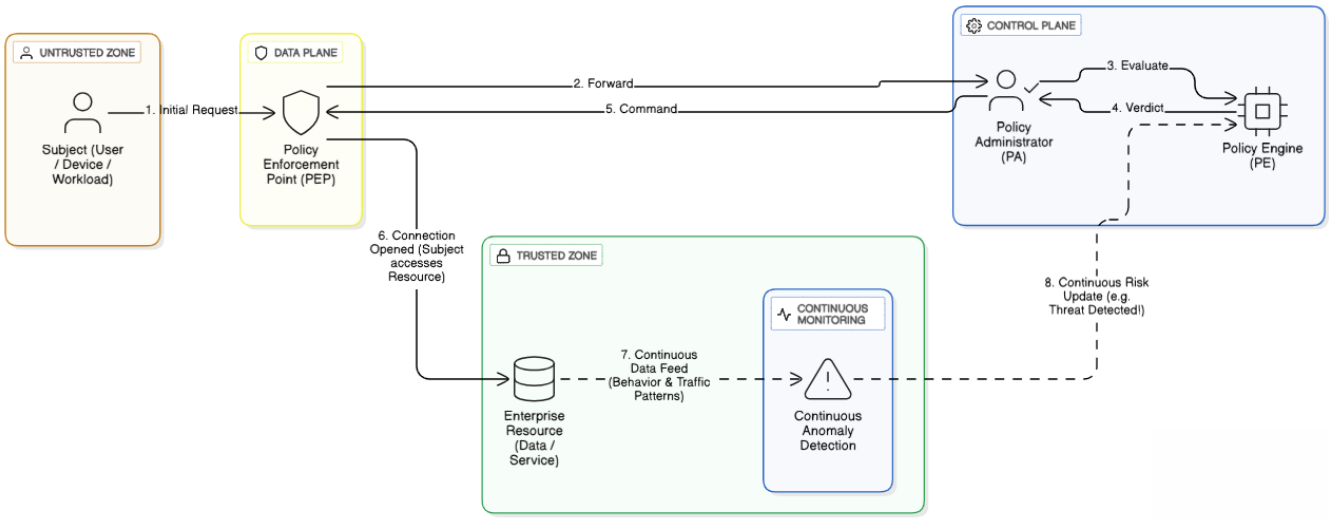

Fig. 2. Zero-Trust data and control plane interaction: the Policy Enforcement Point (PEP) mediates initial requests, the Policy Administrator (PA) and Policy Engine (PE) evaluate and issue decisions, and continuous monitoring feeds post-access anomaly detection back into dynamic risk updates.

expensive. Training a CNN or LSTM on gigabits of real-time traffic requires substantial GPU resources, which may not be available on edge devices or standard enterprise firewalls. Furthermore, ”feature engineering” remains a bottleneck. Huang et al. [23] explore the use of Markov Chains for IoT traffic, noting that the selection of features (e.g., inter-arrival time vs. packet size) drastically changes model performance. There is no universal consensus in the literature on the ”perfect” set of features for encrypted traffic analysis, leaving it an active area of research.

IV. The ”Black Box” Dilemma and Explainable AI (XAI)

A. The Trust Deficit in Automated Security

The central tension identified in this review is between the performance of DL models and their trustworthiness. Venkataramanan [24] argues that in cybersecurity, a false positive is not just a statistical error; it is an operational disruption. If an AI model blocks a CEO’s laptop because it misidentified a legitimate encrypted video call as data exfiltration, the security team needs to know why to prevent a recurrence.

Black-box models (like Deep Neural Networks) offer no such insight. They provide a probability score (e.g., ”99% Malicious”) but no semantic context. This opacity is incompatible with the ”Verify” component of Zero-Trust. As noted earlier by Nazat et al. [10], to ”verify” implies to understand and validate, actions that are impossible with an uninterpretable model.

B. XAI Techniques in Cybersecurity

Researchers are adapting Explainable AI (XAI) techniques from the broader ML field to cybersecurity.

SHAP (SHapley Additive explanations): This is the most widely cited technique in the reviewed papers. Singh et al. [25] develop an ”Interpretable Anomaly Detection” system for encrypted traffic using SHAP and XGBoost with 99.94% accuracy. Similarly, Zeleke et al. [26] use SHAP with Random Forests to detect malware, showing that XAI can highlight if a detection was driven by a specific feature, allowing analysts to validate threats.

LIME vs. SHAP: Nazat et al. [10] perform a comparative analysis and find that SHAP provides consistent global explanations, while LIME is faster for ”local” event-specific explanations, which benefits real-time applications.

Neurosymbolic AI: Kalutharage et al. [9] combine neural networks with symbolic logic (knowledge graphs), mapping detected anomalies to security tactics from frameworks like MITRE ATT&CK.

C. XAI for Policy Enforcement

The literature is beginning to explore using XAI to drive policy changes directly, not just assist analysts. Haque et al. [27] propose a framework where XAI outputs dynamically affect trust scores. Privacy still remains a concern when using metadata for explanations [28], [29].

V. Critical Analysis and Synthesis

A. Methodology vs. Reality

Critical evaluation shows a gap between academic experiments and real-world conditions. Many studies rely on static

datasets like CIC-Darknet2020, CSE-CIC-IDS2018, or CTU-13 [25], [26], [30]. These may not reflect the complexity of recent traffic, such as HTTP/3 or sophisticated ransomware evasion.

A "real-time" fallacy exists: calculating SHAP values for all traffic is computationally heavy. As noted by Prasath and Ruth [31], real-time capability is claimed but rarely achieved. Hybrid solutions—using light screening with heavy explanation only for ambiguous flows—are rarely implemented.

B. The Gap in Integrated Frameworks

The most significant finding from this review is the fragmentation of the field. The literature can be broadly categorized into three silos:

- **Pure ETA Papers:** Focus on optimizing CNNs/LSTMs for accuracy, often ignoring interpretability [19], [20], [32].
- **Pure ZTA Paperss:** Focus on architectural diagrams and policy definitions, often assuming the existence of perfect threat detection [4], [5], [29].
- **Pure XAI Papers:** Focus on the mathematics of interpretability, often using generic datasets rather than complex encrypted network traffic [33], [34].

Very few papers attempt to build a holistic system that integrates all three. Singh et al. [25] come closest, but even they focus primarily on the detection mechanism rather than the downstream Zero-Trust policy enforcement. Other works, such as those by Janiesch et al. [35] and Abououf et al. [36], discuss AI advances broadly or in specific niches (healthcare), but do not bridge the gap to enterprise encrypted traffic enforcement.

C. Research Gap Identification

Based on the synthesis, the following research gaps are noted:

- **Automated Policy Translation:** Mechanisms to directly use XAI outputs for machine-readable ZTA policies (like XACML or OPA rules) are lacking. Analysts, not network systems, are the current consumers of XAI.
- **Efficiency in High-Bandwidth Environments:** Current XAI solutions are not ready for 10 Gbps+ networks. There is a need for "Lightweight XAI" that can keep up with traffic volume.
- **Adversarial XAI:** Few address how adversaries might manipulate features to fool both detection and explanation stages.

D. Comparative Analysis of Existing Approaches

This subsection consolidates the surveyed work into a structured overview; Tables I and II summarize representative techniques across encrypted traffic analysis, Zero Trust, healthcare and IoT security, and XAI, highlighting their main advantages and limitations.

VI. Conclusion

The combination of Zero-Trust Architecture, Encrypted Traffic Analysis, and Explainable AI (XAI) represents the newest and most advanced area of modern network security. This literature review shows that each part has grown strong on its own—Deep Learning can analyze encrypted traffic effectively, and Zero-Trust can secure network systems. However, putting them together is still difficult because of the "Black Box" problem in AI models. The reviewed papers clearly show that Explainable AI is the missing piece needed to make AI-based detection usable in a Zero-Trust system. Without XAI, automatic blocking is too dangerous because we do not know why the model made a decision. With XAI, security decisions become clear, understandable, and easier to defend. The identified research gaps—especially the lack of real-time, automatic policy creation from XAI outputs—give a clear direction for this final year project. By building a framework that not only finds anomalies in hidden (encrypted) traffic but also explains the reason, this project aims to offer a practical solution to one of the most important challenges in cybersecurity today.

VII. Declaration of Writing Assistance

This work benefited from grammatical clarity, rephrasing, and summarization assistance using AI tools including Perplexity, Gemini, ChatGPT-4, Scispace, ChatGPT-5, and Consensus AI for identifying related research papers. Gemini was also used to generate initial versions of illustrative figures, which were then carefully reviewed, edited, and corrected manually to ensure accuracy and alignment with the authors' intended concepts. All technical content, analysis, figures, and conclusions presented in this literature review are solely the authors' original work and have been critically evaluated prior to submission.

References

[1] I. H. Ji, J. H. Lee, M. J. Kang, W. J. Park, S. H. Jeon, and J. T. Seo, "Artificial intelligence-based anomaly detection technology over encrypted traffic: A systematic literature review," *Sensors*, vol. 24, p. 898, 01 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/3/898

[2] S. Han, Q. Wu, H. Zhang, and B. Qin, "Light-weight unsupervised anomaly detection for encrypted malware traffic," vol. 147, pp. 206–213, 07 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9900159

[3] J. Xing and C. Wu, "Detecting anomalies in encrypted traffic via deep dictionary learning," 07 2020.

[4] P. Dhiman, N. Saini, Y. Gulzar, S. Turaev, A. Kaur, K. U. Nisa, and Y. Hamid, "A review and comparative analysis of relevant approaches of zero trust network model," *Sensors*, vol. 24, p. 1328, 01 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/4/1328

[5] S. Sarkar, "Security of zero trust networks in cloud computing: A comparative review," *Sustainability*, vol. 14, p. 11213, 01 2022. [Online]. Available: https://www.mdpi.com/2071-1050/14/18/11213/htm

[6] D. Kodi, "Zero trust in cloud computing: An ai-driven approach to enhanced security," *International Journal of Computer Science and Engineering*, vol. 12, pp. 1–8, 04 2025.

[7] M.-G. Kim and H. Kim, "Anomaly detection in imbalanced encrypted traffic with few packet metadata-based feature extraction," *Computer Modeling in Engineering & Sciences*, vol. 141, pp. 585–607, 01 2024.

[8] H. Liu and H. Wang, "Real-time anomaly detection of network traffic based on cnn," *Symmetry*, vol. 15, p. 1205, 06 2023. [Online]. Available: https://www.mdpi.com/2073-8994/15/6/1205

TABLE I
SUMMARY OF EXISTING TECHNIQUES, ADVANTAGES, AND DISADVANTAGES (PART I)

Domain	Ref.	Technique Used	Key Advantage	Key Disadvantage
Systematic Review	[1]	Systematic Literature Review (SLR)	Provides a comprehensive roadmap of current AI methods and datasets for encrypted traffic.	Does not propose a new detection model; depends on the quality of existing studies.
Encrypted Traffic	[2]	Light-weight Unsupervised Learning	Can detect zero-day (unknown) malware without labelled training data; computationally efficient.	Unsupervised models often suffer from higher false-positive rates than supervised ones.
	[3]	Deep Dictionary Learning (DDL)	Reconstructs complex high-dimensional traffic patterns and identifies anomalies effectively.	Dictionary learning is computationally expensive during training.
	[7]	Few-packet Metadata Extraction	Effective on highly imbalanced datasets using only minimal packet headers.	Relies heavily on metadata; obfuscated headers reduce detection performance.
	[8]	Real-time CNN	CNNs capture spatial correlations in traffic bytes and can be optimised for speed.	Truly real-time operation requires significant hardware acceleration (e.g., GPUs).
	[20]	Parallel Auto–Feature Extraction	Uses parallel processing to speed up feature extraction from encrypted tunnels.	Architecture is complex to implement and consumes substantial resources.
	[21]	Hybrid Deep Learning (CNN+LSTM)	Combines spatial and temporal analysis for higher accuracy.	Training hybrid models is slow and requires large datasets.
Zero Trust	[4]	Comparative Analysis of ZTA	Compares multiple ZTA models to guide organizational adoption.	Primarily theoretical; lacks live performance evaluation.
	[5]	Cloud-based Zero Trust Review	Targets ZTA for dynamic cloud environments.	Managing ZTA is difficult due to ephemeral containers and VMs.
	[6]	AI-driven Zero Trust	Uses AI to automate the ”verify explicitly” principle.	Model drift can lead to false positives that block legitimate users.
	[11]	Cost-effectiveness Analysis	Evaluates financial and resource cost of implementing ZTA.	Focuses on economics rather than technical detection performance.
	[12]	AI + ZTA for Cloud APIs	Secures API endpoints, common attack vectors in cloud applications.	API security differs from network-layer security and needs specialised logs.
	[13]	Threat Intelligence + ZTA	Enriches ZTA decisions with external threat feeds.	Effectiveness depends on quality and latency of the threat intelligence.
	[14]	SDN-based Zero Trust	Implements ZTA using SDN for centralised control.	SDN controller becomes a single point of failure if compromised.
	[18]	Multi-cloud ZTA Performance	Analyses ZTA performance across different cloud providers.	Cross-cloud latency can degrade user experience.
	[24]	AI-powered ZTA Review	Reviews how AI enhances continuous verification in ZTA.	Highlights the black-box problem where AI decisions are hard to audit.
	[29]	AI-enabled ZTA (IIoT)	Targets industrial environments where uptime is critical.	Proprietary industrial protocols are hard to model with standard AI.
Healthcare / IoT / Cloud	[15]	GenAI + Behavioural Biometrics	Uses generative AI and user behaviour for strong identity verification.	Raises privacy concerns over collection of behavioural biometric data.
	[16]	AI Threat Detection (Cloud)	Protects patient data in cloud environments using AI-based detection.	Regulations such as HIPAA/GDPR restrict data available for AI training.
	[17]	Anomaly-based Detection (ML)	Focuses on smart-health devices and sensors.	Resource-constrained IoT devices struggle to run complex models on-device.
	[23]	Anomaly Detection for IoMT	Specifically targets Internet of Medical Things deployments.	High sensitivity is required; false negatives can endanger patient safety.
Cloud Security	[19]	Traffic Packet-based Detection	Analyses raw packet behaviour in cloud environments.	Deep encryption (e.g., TLS 1.3) hides many headers, hindering analysis.
Telecom	[22]	AI in Telecom Review	Examines AI for large-scale telecom networks.	Telecom-specific constraints may not generalise to enterprise networks.

TABLE II
SUMMARY OF EXISTING TECHNIQUES, ADVANTAGES, AND DISADVANTAGES (PART II)

Domain	Ref.	Technique Used	Key Advantage	Key Disadvantage
Explainable AI / XAI	[10]	XAI for Autonomous Systems	Applies XAI to explain anomalies in autonomous driving systems.	High-speed contexts mean XAI calculations add latency.
	[25]	SHAP with Machine Learning	Uses SHAP values to interpret why encrypted traffic is flagged.	SHAP computations are computationally very expensive and slow.
	[26]	XAI for Malware Detection	Explains malware classification decisions in network traffic.	Explanations may be misinterpreted by non-expert analysts.
	[31]	XAI in Simulated Environment	Evaluates XAI tools in controlled simulations.	Simulation results may not fully reflect real network conditions.
	[36]	XAI for Healthcare Monitoring	Explains anomalies in patient monitoring systems.	Even with XAI, accuracy is critical and explanations do not guarantee correctness.
Other Security Domains	[27]	Deep Learning + XAI for UAV Security	Applies ZTA and deep learning with XAI to secure UAVs.	UAVs have strict power and compute limits; heavy models drain batteries.
	[28]	Data-driven Network Analysis	Uses statistical analysis of sensor data for anomaly detection.	Statistical thresholds may miss low-and-slow attacks that mimic normal traffic.
	[30]	Intrusion Analysis with ZTA	Integrates IDS capabilities into a ZTA framework.	Integrating legacy IDS with modern ZTA is architecturally challenging.
General AI / Overview	[32]	ML for Threat Detection	Uses standard ML to detect threats that bypass static ZTA rules.	Requires frequent retraining to handle evolving attack vectors.
	[35]	ML and DL Overview	Provides a broad survey of ML/DL techniques and markets.	Too generic; lacks concrete network-security implementation details.

[9] C. S. Kalutharage, X. Liu, and C. Chrysoulas, "Neurosymbolic learning and domain knowledge-driven explainable ai for enhanced iot network attack detection and response," *Computers & Security*, vol. 151, p. 104318, 01 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404825000070?via=ihub

[10] S. Nazat, L. Li, and M. Abdallah, "Xai-ads: An explainable artificial intelligence framework for enhancing anomaly detection in autonomous driving systems," *IEEE access*, pp. 1–1, 01 2024.

[11] Z. Adahman, A. W. Malik, and Z. Anwar, "An analysis of zero-trust architecture and its cost-effectiveness for organizational security," *Computers & Security*, vol. 122, 09 2022.

[12] L. Micheal, "Integrating ai-powered anomaly detection with zero-trust authorization for cloud apis lee micheal," 03 2025. [Online]. Available: https://www.researchgate.net/publication/394789667_Integrating_AI-Powered_Anomaly_Detection_with_Zero-Trust_Authorization_for_Cloud_APIs_Lee_Micheal

[13] N. S. Kommera, "Enhancing zero trust architecture with ai-driven threat intelligence in cloud environments," *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, vol. 11, pp. 1524–1533, 02 2025. [Online]. Available: https://www.researchgate.net/publication/388829344_Enhancing_Zero_Trust_Architecture_with_AI-Driven_Threat_Intelligence_in_Cloud_Environments

[14] X. Guo, H. Xian, T. Feng, Y. Jiang, D. Zhang, and J. Fang, "An intelligent zero trust secure framework for software defined networking," *ProQuest*, 11 2023. [Online]. Available: https://www.proquest.com/docview/2891024391/EDD1D1D634744CDBPQ/3?accountid=38945&sourcetype=ScholarlyJournals

[15] A. M. Ogunmolu, "Leveraging generative ai and behavioral biometrics to strengthen zero trust cybersecurity architectures in healthcare systems," *Journal of Engineering Research and Reports*, vol. 27, pp. 194–213, 05 2025.

[16] A. Gundaboina, "Ai-driven threat detection and response for healthcare: Securing patient data in cloud environments," *Journal of Engineering and Applied Sciences Technology*, pp. 1–7, 04 2025.

[17] M. Tabassum, S. Mahmood, A. Bukhari, B. Alshemaimri, A. Daud, and F. Khalique, "Anomaly-based threat detection in smart health using machine learning," *BMC medical informatics and decision making*, vol. 24, p. 347, 19 2024. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/39563355/

[18] S. Rodigari, D. O'Shea, P. McCarthy, M. McCarry, and S. McSweeney, "Performance analysis of zero-trust multi-cloud," IEEE Xplore, p. 730–732, 09 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9582229

[19] X. Yin, L. Wu, Y. Zhang, M. Zhang, and Y. Meng, "Anomaly detection based on traffic packets in cloud environment," *2023 IEEE 3rd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA)*, pp. 916–919, 05 2023.

[20] G. Long and Z. Zhang, "Deep encrypted traffic detection: An anomaly detection framework for encryption traffic based on parallel automatic feature extraction," *Computational Intelligence and Neuroscience*, vol. 2023, p. e3316642, 03 2023. [Online]. Available: https://www.hindawi.com/journals/cin/2023/3316642/

[21] T. Bakhshi and B. Ghita, "Anomaly detection in encrypted internet traffic using hybrid deep learning," *Security and Communication Networks*, vol. 2021, pp. 1–16, 09 2021.

[22] E. Edozie, A. N. Shuaibu, B. O. Sadiq, and U. K. John, "Artificial intelligence advances in anomaly detection for telecom networks," *Artificial Intelligence Review*, vol. 58, 01 2025.

[23] H.-C. Huang, I.-H. Liu, M.-H. Lee, and J.-S. Li, "Anomaly detection on network traffic for the healthcare internet of things," 11 2023.

[24] K. S. Sandhu, S. Venkataramanan, V. Kumar, and S. Thota, "Ai-powered anomaly detection in zero trust environments: A comprehensive review of methods and evaluation," *Nanotechnology Perceptions*, vol. 20, pp. 2634–2654, 12 2024. [Online]. Available: https://www.researchgate.net/publication/389634535_AI-Powered_Anomaly_Detection_in_Zero_Trust_Environments_A_Comprehensive_Revie_of_Methods_and_Evaluation

[25] K. Singh, A. Kashyap, and A. K. Cherukuri, "Interpretable anomaly detection in encrypted traffic using shap with machine learning models," *arXiv (Cornell University)*, 05 2025.

[26] S. N. Zeleke, A. F. Jember, and M. Bochicchio, "Integrating explainable ai for effective malware detection in encrypted network traffic," 01 2025. [Online]. Available: https://www.researchgate.net/publication/387873114_Integrating_Explainable_AI_for_Effective_Malware_Detection_in_Encrypted_Network_Traffic

[27] E. Haque, K. Hasan, I. Ahmed, M. S. Alam, and T. Islam, "Enhancing uav security through zero trust architecture: An advanced deep learning and explainable ai analysis," *2016 International Conference on Computing, Networking and Communications (ICNC)*, pp. 463–467, 02 2024.

[28] S. Alam, Y. Alam, S. Cui, and C. M. Akujuobi, "Data-driven network analysis for anomaly traffic detection," *Sensors*, vol. 23, pp. 8174–8174, 09 2023.

[29] A. A. Laghari, A. A. Khan, A. Ksibi, F. Hajjej, N. Kryvinska, A. Almadhor, M. A. Mohamed, and S. Alsubai, "A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture," *Scientific Reports*, vol. 15, 07 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-11738-9

[30] N. Gautam, H. Mishra, and A. Singh, "Network traffic analysis for intrusion with zero-trust," *International Research Journal of Modernization in Engineering Technology and Science*, 06 2024.

[31] "Network traffic analysis and anomaly detection in a simulated environment using explainable ai," *International Research Journal of Modernization in Engineering Technology and Science*, 08 2024.

[32] L. Gudala, M. Shaik, and S. Venkataramanan, "Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: An exploration of real-time anomaly identification and adaptive mitigation strategies," *Journal of Artificial Intelligence Research*, vol. 1, p. 19–45, 11 2021. [Online]. Available: https://thesciencebrigade.com/JAIR/article/view/222

[33] S. Tariyal, A. Majumdar, R. Singh, and M. Vatsa, "Greedy deep dictionary learning," *arXiv (Cornell University)*, 01 2016.

[34] A. Ikram, "Zero trust architecture for healthcare: Reinventing cybersecurity in the age of ai and iot-driven patient data," *Iconic Research And Engineering Journals*, vol. 8, pp. 1523–1534, 06 2025. [Online]. Available: https://www.irejournals.com/paper-details/1709404

[35] C. Janiesch, P. Zschech, and K. Heinrich, "Machine learning and deep learning," 04 2021. [Online]. Available: https://www.researchgate.net/publication/350834453_Machine_learning_and_deep_learning

[36] M. Abououf, S. Singh, R. Mizouni, and H. Otrok, "Explainable ai for event and anomaly detection and classification in healthcare monitoring systems," *IEEE Internet of Things Journal*, pp. 1–1, 01 2023.