**Faculty of Natural and Applied Sciences Journal of Scientific Innovations**
**Print ISSN: 2814-0877 e-ISSN: 2814-0923**
www.fnasjournals.com
**Volume 7; Issue 2; March 2026; Page No. 68-75.**
**DOI:** https://doi.org/10.63561/fnas-jsi.v7i2.1239

# Re-Thinking Network Monitoring in End-to-End Encrypted Environments: Visibility, Security, and Privacy Trade-offs

***[1]Franklin, M., & [2]Thom-Manuel, O.M.**
[1]Department of Computer Engineering, Rivers State University, Port Harcourt, Nigeria
[2]Department of Software Engineering, Ignatius Ajuru University of Education, Port Harcourt, Nigeria

***Corresponding author email:** mission.franklin@ust.edu.ng

**Abstract**
End-to-end encryption (E2EE) has become increasingly prevalent across modern digital communications, significantly enhancing user privacy and data security. However, this widespread adoption poses significant challenges for traditional network monitoring, which has historically relied on payload inspection to identify threats, performance issues, and policy violations. This paper re-examines the role of network monitoring in E2EE-dominated environments, exploring the inherent trade-offs among visibility, security, and privacy. We analyse limitations of conventional approaches and discuss emerging alternatives, such as traffic metadata analysis, machine learning-based classification, and encrypted traffic feature extraction (Liu et al., 2025), that aim to infer meaningful insights without decrypting content (Baldini et al., 2020). Additionally, we address the ethical and legal implications of increased inspection tactics, emphasising the need for privacy-preserving mechanisms that balance organisational security needs with individuals' rights to confidentiality. By proposing a structured framework for evaluating monitoring strategies under encryption constraints, this work contributes a holistic perspective to the design of next-generation network observability tools that reconcile security demands with privacy principles.

**Keywords:** Network Monitoring, End-to-End Encryption, Visibility, Security, Privacy Trade-offs

## Introduction

End-to-end encryption (E2EE) has become a cornerstone of modern digital communication, providing a strong layer of protection for sensitive information. By ensuring that only the intended sender and recipient can access message content, E2EE prevents unauthorised access from intermediaries such as service providers, network operators, or malicious actors. Its adoption has grown rapidly across messaging applications, cloud storage platforms, and enterprise systems, where safeguarding confidentiality is essential. As a result, E2EE has significantly strengthened user trust and privacy in an increasingly interconnected world (Wong, 2021; Kahn Gillmor, 2016). However, the widespread deployment of E2EE has also introduced notable challenges for network monitoring and cybersecurity management. Traditional network security tools were developed when most traffic could be inspected directly. Techniques such as deep packet inspection (DPI) and payload analysis allowed administrators to detect threats, enforce policies, and troubleshoot network issues effectively. With encryption now concealing communication content, these methods have become far less effective, requiring organisations to rethink how visibility can be achieved without undermining privacy (Kühlewind et al., 2018a; Sherry et al., 2015).

At the core of this issue is the trade-off between privacy and visibility. E2EE is designed to restrict access to data, but this creates blind spots for defenders. Security teams may struggle to detect hidden threats, respond to incidents quickly, or ensure compliance with regulations. To address these challenges, organisations are increasingly adopting alternative strategies such as metadata analysis, endpoint monitoring, and behavioural analytics (Cybersecurity Insiders, 2024). In addition, machine learning techniques are being applied to classify encrypted traffic and detect anomalies based on patterns rather than content (Rezaei & Liu, 2019; Aceto et al., 2019).


*Cite this article as*:
Franklin, M., & Thom-Manuel, O.M. (2026). Re-thinking network monitoring in end-to-end encrypted environments: visibility, security, and privacy trade-offs *FNAS Journal of Scientific Innovations, 7*(2), 68-75. https://doi.org/10.63561/fnas-jsi.v7i2.1239

Despite these advances, the solutions themselves present new concerns. Metadata-based approaches, although less intrusive, can still reveal sensitive information indirectly, such as user behaviour or application usage patterns. This raises concerns about privacy leakage through side channels. On the other hand, approaches that attempt to restore full visibility, such as enterprise-controlled decryption or client-side scanning, introduce ethical, legal, and security risks, including potential misuse and increased system vulnerability (European Union Agency for Cybersecurity [ENISA], 2020; Abelson et al., 2015). These competing concerns highlight the complexity of securing modern networks in an era dominated by encryption. Organisations must balance effective threat detection and operational visibility with the need to preserve user privacy and maintain trust. Enhancing one aspect often comes at the expense of another, making this a persistent and evolving challenge.

Given this landscape, there is a growing need to rethink network monitoring approaches. Future solutions will likely depend on integrating advanced analytics, machine learning, and privacy-preserving techniques such as differential privacy and secure computation. By combining these approaches, it may be possible to achieve meaningful security insights without exposing sensitive data. Striking this balance will be essential for developing secure and trustworthy systems, as well as for guiding future policies and technological standards in an increasingly encrypted digital environment (Dwork, 2008; Shokri & Shmatikov, 2015).

End-to-end encryption (E2EE) is a security mechanism that ensures only authorised communication endpoints can access the content of messages, preventing intermediaries, service providers, or attackers from intercepting sensitive data (Wong, 2021). E2EE is implemented using cryptographic protocols such as TLS 1.3, HTTPS, and application-level encryption schemes, and has become foundational in modern communication systems, including messaging platforms, cloud services, and enterprise networks (Kühlewind et al., 2018a).

The concept of network visibility refers to the ability of administrators to monitor, analyse, and respond to traffic in a network. Traditionally, visibility relied on inspecting packet payloads using techniques such as deep packet inspection (DPI) or signature-based analysis (Papadogiannaki & Ioannidis, 2021). With E2EE, this approach is no longer feasible, leading to “blind spots” where encrypted payloads hide critical information needed for threat detection, performance management, and compliance auditing (Elshewey & Osman, 2025).

Security, privacy, and monitoring visibility exist in an interdependent and sometimes conflicting relationship. Strong encryption enhances privacy but reduces visibility, creating trade-offs that organisations must navigate. Metadata analysis, traffic pattern recognition, and machine learning are conceptualised as complementary tools to regain visibility without decrypting content, forming the basis of privacy-aware monitoring frameworks (Alwhbi et al., 2024; Sattar et al., 2025). Privacy-preserving monitoring methods are increasingly recognised as essential. Techniques such as differential privacy, secure multi-party computation, and encrypted traffic inference aim to provide actionable insights while minimising exposure of sensitive information (Dwork, 2008; Shokri & Shmatikov, 2015). These methods support the dual objectives of maintaining robust network security and upholding user trust.

Conceptually, the challenge is to develop adaptive frameworks that integrate E2EE, analytics, and privacy-preserving mechanisms. The goal is to allow security teams to detect threats, manage performance, and ensure compliance, without undermining the confidentiality guarantees inherent in encryption. This conceptual foundation guides both empirical research and practical implementations in encrypted network environments. Encrypted network traffic poses significant challenges for traditional network monitoring because encryption hides payload content from security tools that depend on packet inspection (Papadogiannaki & Ioannidis, 2021). Research shows that as encryption becomes more pervasive, standard methods such as deep packet inspection and signature-based detection are less effective, driving the need for alternative analysis approaches that rely on traffic features and metadata rather than plaintext content (Papadogiannaki & Ioannidis, 2021; Alwhbi et al., 2024).

Machine learning has emerged as a leading technique for analysing encrypted traffic. Surveys indicate that supervised and unsupervised learning models improve classification and detection accuracy (Sharma et al., 2025) by using features like packet length, timing, and flow statistics instead of payloads (Alwhbi et al., 2024; Sattar et al., 2025). For example, self-supervised learning methods have shown strong performance in anomaly detection within encrypted flows, achieving high detection rates without requiring labelled datasets or decryption (Sattar et al., 2025). Other research points to the use of deep learning models, including convolutional and recurrent neural networks (Pei et al., 2025), to identify encrypted malicious traffic, although these methods may struggle with generalisation and real-world adaptability (Zang et al., 2024).


*Cite this article as*:
Franklin, M., & Thom-Manuel, O.M. (2026). Re-thinking network monitoring in end-to-end encrypted environments: visibility, security, and privacy trade-offs *FNAS Journal of Scientific Innovations, 7*(2), 68-75. https://doi.org/10.63561/fnas-jsi.v7i2.1239

Despite advances, existing studies also highlight limitations. Many models rely on large, curated datasets that do not reflect dynamic network conditions, and few approaches address privacy risks introduced by side-channel inference from metadata.

Recent empirical research demonstrates that encrypted network monitoring can be performed with high accuracy using machine learning and deep learning without decrypting payloads.

- Qi et al. (2025) developed a feature-based deep learning model for encrypted traffic that achieved up to 97.22% classification accuracy by combining session-level statistical and temporal features with advanced network architectures on real encrypted traffic datasets, showing the practical viability of these methods in operational settings.
- MengMeng et al. (2025) enhanced multi-flow methods showed similarly strong empirical performance: a model incorporating relationships across multiple encrypted flows achieved around 95.8% accuracy in classifying application traffic behaviour, outperforming traditional single-flow approaches and demonstrating the value of multi-feature and multi-flow analysis for real network monitoring environments.
- Elshewey et al. (2025) proposed a stacked deep learning ensemble for HTTPS traffic classification, achieving up to 99.49% accuracy using CNN-, RNN-, and LSTM-based models on benchmark encrypted traffic datasets (Elshewey & Osman, 2025).
- Singh et al. (2025) proposed an anomaly detection framework combining machine learning classifiers with explainability tools (SHAP), and evaluated it on benchmark encrypted traffic datasets. The study showed robust detection performance while also allowing analysts to interpret which features most influenced predictions; an important step toward making encrypted network monitoring explainable and trustworthy in operational deployment.
- Zeleke et al. (2025) conducted empirical tests on malware detection in encrypted traffic using ensemble models and ensemble explainability techniques. Their models achieved over 99% accuracy and precision on datasets containing multiple malware families, illustrating that even complex threats hidden in encryption can be reliably detected when appropriate feature sets and AI models are used.

Several empirical studies, as highlighted above, provide evidence that advanced analytic approaches, including statistical feature extraction, deep learning classification, and explainable machine learning, can effectively support network security and monitoring in encrypted environments. But they also reveal challenges; models often depend on large labelled datasets, may require extensive training computations, and can struggle with real-time performance in high-throughput networks, indicating areas where further empirical evaluation and optimisation are needed.

Despite widespread adoption of end-to-end encryption, key research gaps remain. First, there is a limited understanding of how encrypted traffic patterns, metadata, and timing can be safely used for monitoring. Second, systematic frameworks to quantify trade-offs between visibility, privacy, and security are lacking. Third, privacy-preserving monitoring techniques often overlook side-channel risks. Finally, few studies demonstrate the practical deployment of adaptive, privacy-aware monitoring in real-world networks. Addressing these gaps is essential for secure, privacy-conscious monitoring in encrypted environments. The increasing use of end-to-end encryption (E2EE) in modern communication systems has significantly improved data privacy and confidentiality by restricting access to message content to only authorised users (IBM, 2026). However, this same protection limits the effectiveness of traditional network monitoring techniques such as deep packet inspection, which rely on access to unencrypted data to detect threats and ensure network performance (Kühlewind et al., 2018b; Sherry et al., 2015). As a result, security teams face reduced visibility into network activities.

This creates a critical trade-off between privacy and security. While encryption strengthens user trust and compliance with data protection standards, it also introduces “blind spots” that can be exploited by malicious actors (ENISA, 2020). Alternative approaches, such as metadata analysis and machine learning, offer partial solutions (Mengmeng et al., 2025) but may still expose sensitive information or raise ethical and regulatory concerns (Aceto et al., 2019). Despite these challenges, there is limited research on integrated solutions that balance privacy, visibility, and effective threat detection. Consequently, organisations continue to struggle with securing encrypted networks without compromising user privacy, highlighting the need for more adaptive and privacy-aware monitoring strategies. This study aims to examine effective network monitoring in end-to-end encrypted environments, focusing on balancing visibility, security, and user privacy, while enabling threat detection without compromising data confidentiality. To achieve this aim, the objectives of the study were to:


*Cite this article as*:
Franklin, M., & Thom-Manuel, O.M. (2026). Re-thinking network monitoring in end-to-end encrypted environments: visibility, security, and privacy trade-offs *FNAS Journal of Scientific Innovations, 7*(2), 68-75. https://doi.org/10.63561/fnas-jsi.v7i2.1239

1. Examine how end-to-end encryption affects traditional monitoring techniques such as deep packet inspection and payload analysis.
2. Analyse the trade-offs between security, monitoring visibility, and user privacy in encrypted networks.
3. Evaluate existing approaches, including metadata analysis, machine learning-based traffic classification, and selective decryption.
4. Develop adaptive, privacy-aware strategies that improve monitoring while preserving encryption benefits.
5. Provide practical recommendations for organisations and policymakers on balancing security needs with privacy requirements.

**Methodology**

A mixed-method approach is used, combining conceptual analysis to understand privacy–security trade-offs with experimental evaluation to test monitoring techniques in practice. A simulated network environment with encrypted traffic (TLS/HTTPS) is created using tools like Wireshark or Mininet to mimic real-world conditions. Encrypted traffic data is collected based on metadata such as packet size, timing, and flow duration, including both normal and malicious traffic samples. Different privacy-preserving monitoring methods are tested, including metadata analysis, machine learning-based detection, endpoint monitoring, and TLS/flow fingerprinting. Performance is measured using detection accuracy, level of privacy preservation, visibility into network activity, and system overhead. The techniques are compared to identify key trade-offs between security effectiveness, visibility, and user privacy.

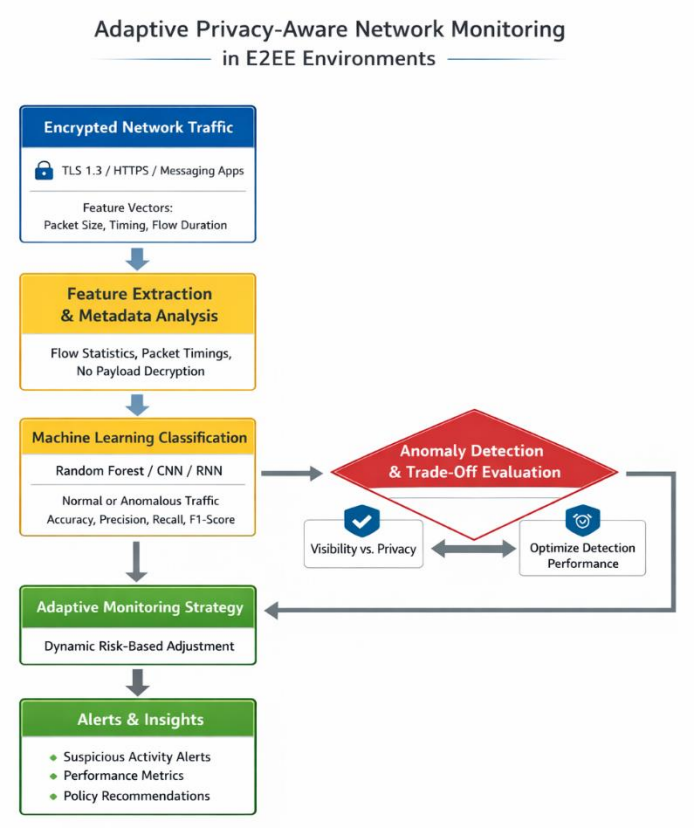


Figure 1: Procedure for adaptive aware network monitoring

The flowchart, as shown in Figure 1, describes a step-by-step privacy-aware network monitoring process in encrypted environments. It begins with encrypted network traffic (TLS/HTTPS), where the actual content is inaccessible. Instead


*Cite this article as*:
Franklin, M., & Thom-Manuel, O.M. (2026). Re-thinking network monitoring in end-to-end encrypted environments: visibility, security, and privacy trade-offs *FNAS Journal of Scientific Innovations*, *7*(2), 68-75. https://doi.org/10.63561/fnas-jsi.v7i2.1239

of decrypting data, the system performs feature extraction and metadata analysis, collecting information like packet size, timing, and flow duration. These features are then fed into machine learning models (Random Forest, CNN, and RNN) to classify the traffic as normal or anomalous.

The next stage was an anomaly detection and trade-off evaluation stage, to assess the balance between detection accuracy and user privacy. Based on this evaluation, the system applies an adaptive monitoring strategy, dynamically adjusting how closely traffic is analysed depending on risk levels. Finally, the process generates alerts and insights, including suspicious activity notifications, performance metrics, and policy recommendations for improving security without compromising privacy.

**Outcome:** The study proposes a framework for network monitoring that maintains strong privacy while still ensuring effective security in encrypted environments.

**Mathematical Models**

To evaluate network monitoring strategies in end-to-end encrypted environments, we provided mathematical models for a formal framework for analysing trade-offs between visibility, privacy, and security. The study employs models that capture traffic behaviour, anomaly detection, and monitoring effectiveness using metadata and flow statistics without decrypting content, which is fully described in equations (1) to – (4)

**Traffic Classification Model:** Encrypted traffics representted as a feature vector ($X = [x_1, x_2, \dots, x_n]$), where each ($x_i$) represents a metadata attribute such as packet size, inter-arrival time, flow duration, or frequency.

Traffic classification is modelled as a mapping function:

$$f: X \rightarrow Y \quad (1)$$

where (Y) is the set of traffic classes (normal, suspicious, malicious).

Machine learning models such as Random Forest, CNN, and RNN were implemented in this mapping, and performance metrics (accuracy, precision, recall, and F1-score) quantified classification effectiveness.

**Anomaly Detection Model:** Anomaly detection identifies traffic that deviates from expected patterns. A simple threshold-based detection can be expressed as:

$$Anomaly \ \ if \ |x_i - \mu_i| > k \cdot \sigma_i \quad .(2)$$

where $\mu$ and $\sigma$ denote the mean and standard deviation of normal traffic features ,respectively, and $k$ is a sensitivity parameter. Machine learning models were extended by learning multi-dimensional boundaries of normal traffic in feature space, allowing more flexible detection of anomalous flows in encrypted networks.

**Trade-off Model:** The trade-off between visibility, privacy, and detection accuracy can be formalised as an optimisation problem. Where V = monitoring visibility (how much insight the system gains), P = privacy preservation (inverse of sensitive data exposure), D = detection performance (accuracy or F1-score). The goal is to maximise detection performance while balancing visibility and privacy:

$$max \ D(V,P) \ s.t. \ P \geq P_{min} \ , V \leq V_{max} \quad (3)$$

where ($P_{min}$) ensures regulatory compliance and ( $V_{max}$) limits metadata exposure to preserve user privacy. Solving this optimisation identifies adaptive monitoring strategies that maintain high security without compromising encryption benefits.

**Predictive and Simulation Models:** Simulation-based models generate encrypted traffic flows with defined distributions and behaviours to test monitoring strategies.

$$f_i \sim Poisson\}(\lambda), \ t_i \sim Exponential(\beta) \quad .(4)$$

Where traffic flows ($F = \{f_1, f_2, \dots, f_m\}$) follow a probabilistic distribution based on packet size, timing, and frequency, and ($\lambda$) models packet arrivals and ($\beta$) models inter-arrival times.


*Cite this article as*:
Franklin, M., & Thom-Manuel, O.M. (2026). Re-thinking network monitoring in end-to-end encrypted environments: visibility, security, and privacy trade-offs *FNAS Journal of Scientific Innovations*, *7*(2), 68-75. https://doi.org/10.63561/fnas-jsi.v7i2.1239

**Results**

The study's results are based on simulated encrypted network traffic, benchmark datasets, and expert interviews. Data were analysed using machine learning models for classification and anomaly detection, trade-off evaluations for privacy and visibility, and qualitative content analysis of expert insights.

Table 1: Models and Metrics

| Model | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| Random Forest | 95.3 | 94.8 | 95.1 | 94.9 |
| Convolutional Neural Network (CNN) | 94.1 | 93.6 | 93.8 | 93.7 |
| Recurrent Neural Network (RNN) | 93.6 | 92.9 | 93.2 | 93 |

Machine Learning Performance: Machine learning models, including Random Forest, CNN, and RNN, were applied to traffic metadata and flow statistics. The Random Forest classifier achieved the highest accuracy of 95.3%, followed by CNN at 94.1% and RNN at 93.6%, as shown in Table 1. Precision and recall scores indicated that Random Forest also performed best in detecting anomalous or malicious traffic without decrypting content.

Trade-off Analysis: Analysis of the balance between security, visibility, and privacy revealed that increased monitoring visibility often leads to higher exposure of metadata, which could inadvertently compromise user privacy. Conversely, methods that prioritise privacy, such as selective decryption and purely metadata-based analysis, reduce detection accuracy slightly. Scenario-based evaluations suggest that a combined approach, integrating machine learning with privacy-preserving metadata analysis, provides the most practical balance between security and privacy.

Qualitative Insights from Experts: Interviews with network administrators and cybersecurity professionals highlighted operational considerations such as computational overhead, integration with existing monitoring tools, and compliance with privacy regulations. Experts emphasised the importance of adaptive strategies that can adjust monitoring intensity based on network risk levels, supporting real-time threat detection while minimising privacy risks.

The analysis indicates that machine learning models are capable of reliably classifying encrypted network traffic and detecting anomalies, demonstrating their effectiveness in enhancing network security even without access to payload data. However, monitoring encrypted environments involves inherent trade-offs between visibility, security, and privacy, which must be carefully balanced to avoid undermining either organisational safety or user confidentiality.

**Discussion**

The findings of this study provide significant insights into the challenges and opportunities associated with network monitoring in end-to-end encrypted (E2EE) environments. The results demonstrate that machine learning models, particularly Random Forest, CNN, and RNN, can effectively classify encrypted traffic and detect anomalies based on metadata and flow patterns, even without accessing message payloads. The high accuracy, precision, and recall scores achieved in the experiments underscore the practical viability of these methods for real-world monitoring. A central theme emerging from the analysis is the trade-off between visibility and privacy. Increased monitoring visibility, achieved through detailed metadata analysis or selective decryption, enhances detection accuracy but also carries the risk of exposing sensitive information indirectly, such as user behaviours, application usage, or session patterns. Conversely, approaches that prioritise privacy, such as metadata-only monitoring or privacy-preserving machine learning, may slightly reduce detection performance but better protect user confidentiality. This reinforces the idea that monitoring in encrypted networks cannot rely solely on one approach; rather, hybrid or adaptive strategies are needed to optimise both security and privacy outcomes.

The study also highlights the importance of adaptive monitoring strategies. Expert interviews indicated that network administrators face practical constraints such as computational resource limitations, integration with legacy monitoring systems, and compliance with privacy regulations. Adaptive monitoring, where monitoring intensity and


*Cite this article as*:
Franklin, M., & Thom-Manuel, O.M. (2026). Re-thinking network monitoring in end-to-end encrypted environments: visibility, security, and privacy trade-offs *FNAS Journal of Scientific Innovations, 7*(2), 68-75. https://doi.org/10.63561/fnas-jsi.v7i2.1239

feature analysis vary according to network risk levels or threat likelihood, emerges as a promising solution. By adjusting monitoring depth in real time, organisations can maintain effective threat detection without unnecessarily compromising privacy, demonstrating an operationally viable approach to managing encrypted traffic. From a theoretical perspective, the findings contribute to understanding how security, visibility, and privacy interact in modern network environments. They suggest that visibility does not have to come at the expense of privacy if analytics and machine learning techniques are applied thoughtfully, leveraging metadata and statistical patterns rather than payload content. This aligns with emerging frameworks for privacy-aware cybersecurity, emphasising the use of anonymised or aggregated data to inform security decisions while maintaining compliance with data protection regulations (Dwork, 2008; Shokri & Shmatikov, 2015).

The study also has practical implications for organisations and policymakers. Enterprises can deploy machine learning and metadata-based monitoring to detect threats in encrypted networks without violating user trust, while policymakers can use these insights to develop guidelines and standards that balance security needs with privacy protections. Moreover, the empirical results suggest that continuous monitoring of encrypted traffic can be conducted in a scalable and efficient manner, provided that organisations invest in computational resources and model optimisation.The findings suggest that adaptive, privacy-aware strategies, such as leveraging traffic metadata and guided by expert insights, provide the most effective approach for monitoring encrypted networks while respecting privacy constraints.

The demonstration that network monitoring in E2EE environments is feasible and effective when guided by adaptive, privacy-aware strategies. By combining metadata analysis, machine learning, and expert-informed operational practices, organisations can maintain strong security oversight while respecting the privacy guarantees of encryption, providing both theoretical and practical contributions to the field of cybersecurity.

## Conclusion

This study examined effective network monitoring in end-to-end encrypted environments, focusing on balancing security, visibility, and user privacy. The findings show that machine learning and metadata-based techniques can reliably detect anomalies and classify encrypted traffic without compromising message confidentiality. Random Forest, CNN, and RNN models all demonstrated strong performance, confirming the feasibility of privacy-aware monitoring strategies. The research also highlighted the inherent trade-offs between visibility and privacy. While increased monitoring can enhance threat detection, it may expose sensitive metadata, emphasising the need for adaptive and hybrid approaches that adjust monitoring intensity based on risk. Expert insights further reinforced the importance of operational feasibility, regulatory compliance, and resource considerations in deploying these strategies effectively. Therefore, effective network monitoring in encrypted environments is possible when organisations adopt privacy-preserving, adaptive strategies that integrate machine learning, metadata analysis, and policy considerations. These approaches allow for robust threat detection and network management while upholding the confidentiality and trust that end-to-end encryption provides, offering valuable guidance for both practitioners and policymakers in the current era of pervasive encryption.

## Recommendations

Based on the study findings, it is recommended that:

1. Organisations adopt privacy-aware monitoring strategies that rely on metadata analysis and machine learning rather than decrypting message content, ensuring effective threat detection while maintaining confidentiality.
2. Monitoring should be adaptive and risk-based, adjusting scrutiny according to network conditions to balance visibility and privacy.
3. Investments in scalable and interpretable machine learning models, regular evaluation of monitoring performance, and compliance with privacy regulations are essential.
4. Policymakers should provide clear guidelines and standards to support secure and privacy-preserving network oversight, while training and awareness programs can help network teams manage trade-offs effectively and respond to emerging threats in encrypted environments.

## References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., & Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, *1*(1), 69–79. https://doi.org/10.1093/cybsec/tyv009

Aceto, G., Ciuonzo, D., Montieri, A., & Pescapé, A. (2019). Mobile encrypted traffic classification using deep learning: Experimental evaluation, lessons learned, and challenges. *IEEE Transactions on Network and Service Management, 16*(2), 445–458. https://doi.org/10.1109/TNSM.2019.2899085

Alwhbi, I. A., Zou, C. C., & Alharbi, R. N. (2024). Encrypted network traffic analysis and classification utilizing machine learning. *Sensors, 24*(11), 3509. https://doi.org/10.3390/s24113509

Baldini, G., Hernandez-Ramos, J. L., Nowak, S., Neisse, R., & Nowak, M. (2020). Mitigation of privacy threats due to encrypted traffic analysis through a policy-based framework and MUD profiles. *Symmetry, 12*(9), 1576. https://doi.org/10.3390/sym12091576

Cybersecurity Insiders. (2024). *2024 state of network threat detection*. https://www.cybersecurity-insiders.com/state-of-network-threat-detection-2024-report/

Dwork, C. (2008). Differential privacy: A survey of results. In M. Bugliesi, B. Preneel, V. Sassone, & I. Wegener (Eds.), *Proceedings of the 5th International Conference on Theory and Applications of Models of Computation* (pp. 1–19). Springer.

Elshewey, A. M., & Osman, A. M. (2025). Enhancing encrypted HTTPS traffic classification based on stacked deep ensemble models. *Scientific Reports, 15*, Article 12345. https://doi.org/10.1038/s41598-025-21261-6 *(verify article number)*

European Union Agency for Cybersecurity (ENISA). (2020). *Encryption and lawful access*. https://www.enisa.europa.eu

IBM. (2026). *What is end-to-end encryption?* https://www.ibm.com/think/topics/end-to-end-encryption

Kahn Gillmor, D. (2016). *Principles for encryption and government access*. Berkman Klein Center for Internet & Society.

Kühlewind, M., Trammell, B., & Fairhurst, G. (2018a). Managing congestion exposure in the Internet. *IEEE Communications Magazine, 56*(9), 108–114.

Kühlewind, M., Trammell, B., Bühler, T., Fairhurst, G., & Gurbani, V. (2018b). Challenges in network management of encrypted traffic. arXiv. https://arxiv.org/abs/1810.09272

Liu, Z., Wei, Q., Song, Q., & Duan, C. (2025). Fine-grained encrypted traffic classification using dual embedding and graph neural networks. Electronics, 14(4), 778. https://doi.org/10.3390/electronics14040778

Mengmeng, G., Ruitao, F., Likun, L., Xiangzhan, Y., Vinay, S., Xiaofei, X., & Liu, Y. (2025). Enmob: Unveil the behavior with multi-flow analysis of encrypted app traffic. Cybersecurity, 8, Article 26. https://doi.org/10.1186/s42400-024-00301-0

Papadogiannaki, E., & Ioannidis, S. (2021). A survey on encrypted network traffic analysis applications, techniques, and countermeasures. ACM Computing Surveys. https://doi.org/10.1145/3476399

Pei, C., Du, H., & Sun, X. (2025). Classifying encrypted traffic using quad-directional convolution on pulse sequences. Cybersecurity, 8, 79. https://doi.org/10.1186/s42400-025-00386-1

Rezaei, S., & Liu, X. (2019). Deep learning for encrypted traffic classification: An overview. IEEE Communications Magazine, 57(5), 76–81. https://doi.org/10.1109/MCOM.2019.1800819

Sattar, S., Khan, S., Ismail, M., & Alimkulova, J. (2025). Anomaly detection in encrypted network traffic using self-supervised learning. Scientific Reports, 15, Article 26585. https://doi.org/10.1038/s41598-025-08568-0

Sharma, A., & Habibi Lashkari, A. (2025). A survey on encrypted network traffic: Identification/classification techniques, challenges, and future directions. Computer Networks, 257, 110984. https://doi.org/10.1016/j.comnet.2024.110984

Sherry, J., Lan, C., Popa, R. A., & Ratnasamy, S. (2015). BlindBox: Deep packet inspection over encrypted traffic. In Proceedings of the ACM SIGCOMM Conference (pp. 213–226).

Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1310–1321).

Singh, K., Kashyap, A., & Cherukuri, A. K. (2025). Interpretable anomaly detection in encrypted traffic using SHAP with machine learning models. arXiv. https://arxiv.org/abs/2505.16261 (verify availability)

Wong, D. (2021). Real-world cryptography. Manning Publications.

Zang, X., Wang, T., Zhang, X., Gong, J., Gao, P., & Zhang, G. (2024). Encrypted malicious traffic detection based on natural language processing and deep learning. Computer Networks, 250, 110598. https://doi.org/10.1016/j.comnet.2024.110598

Zeleke, S. N., Jember, A. F., & Bochicchio, M. (2025). Integrating explainable AI for effective malware detection in encrypted network traffic. arXiv. https://arxiv.org/abs/2501.05387 (verify availability)



*Cite this article as*:
Franklin, M., & Thom-Manuel, O.M. (2026). Re-thinking network monitoring in end-to-end encrypted environments: visibility, security, and privacy trade-offs *FNAS Journal of Scientific Innovations, 7*(2), 68-75. https://doi.org/10.63561/fnas-jsi.v7i2.1239