SRJ: INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

VOLUME 01 | ISSUE 10 OCTOBER 2026	MULTIDISCIPLINARY • PEER-REVIEWED OPEN ACCESS • PAGES 21–25	ISSN (ONLINE): 3139-8758 www.journalsrj.com

ORIGINAL RESEARCH ARTICLE

Article DOI: 10.68295/SRJ/PTBX5261
Article URL: https://doi.org/10.68295/SRJ/PTBX5261

FACTORS ASSOCIATED WITH TRUST IN DEEP-LEARNING-BASED THREAT DETECTION FOR ENCRYPTED DARKNET TRAFFIC

Blessing Thomas Udoh

1. *Research Scholar at Paris American International University, United Arab Emirates (UAE).*

MANUSCRIPT INFO

Received: 23 Aug 2026
Revised: 22 Sep 2026
Final Accepted: 12 Oct 2026
Published: 25 Oct 2026

KEYWORDS

encrypted traffic;
darknet;
deep learning;
cybersecurity;
detection trust;
privacy;
mixed methods

ABSTRACT

Encrypted traffic and anonymity-oriented networks create challenges for cybersecurity monitoring because the content of communications may not be directly inspected. This study examines factors associated with trust in deep-learning-based, real-time threat detection for encrypted darknet traffic, focusing on privacy issues, threat experience, and encryption knowledge. A mixed-method design was used, combining questionnaire responses from 151 participants with seven semi-structured interviews. The questionnaire demonstrated high overall internal consistency (Cronbach's $\alpha = 0.914$). Pearson correlations showed positive associations between Detection Trust and Privacy Issues ($r = 0.547$), Threat Experience ($r = 0.673$), and Encryption Knowledge ($r = 0.682$), with reported p-values below .001. A multiple regression model was statistically significant, $F(3,147) = 70.192$, $p < .001$, and explained 58.9% of the variance in Detection Trust ($R^2 = 0.589$; adjusted $R^2 = 0.581$). Standardised coefficients reported in the thesis were $\beta = 0.187$ for Privacy Issues ($p = .004$), $\beta = 0.341$ for Threat Experience ($p < .001$), and $\beta = 0.377$ for Encryption Knowledge ($p < .001$). Interview analysis identified six themes concerning encrypted-traffic visibility, limitations of conventional tools, the potential of metadata-based deep learning, privacy and ethics, trust and explainability, and real-time implementation requirements. The findings concern participants' perceptions and statistical associations; the study did not experimentally evaluate a deployed deep-learning detector or establish causal effects. The results indicate that trust-oriented system design should address privacy safeguards, transparent explanations, realistic validation, low latency, and continuous performance monitoring.

Corresponding Author: **Blessing Thomas Udoh.**
Research Scholar at Paris American International University, United Arab Emirates (UAE).

© 2026 by the Author(s). Published by SRJ Publication and Research LLP under the Creative Commons Attribution (CC BY) 4.0 License.

1. Introduction

The expansion of encrypted communication and anonymity-focused networks complicates network threat detection. Encryption protects legitimate users' confidentiality, but it also limits direct inspection of packet payloads. Security teams therefore often depend on indirect indicators such as flow duration, packet size, timing, direction, and connection patterns. These indicators can be useful, but benign and malicious activities may share similar observable characteristics, creating risks of false positives and false negatives.

Traditional signature-based approaches can be effective against known patterns but may fail to identify previously unseen or substantially modified attacks. Anomaly-based systems can identify deviations from established behaviour, yet excessive alerts can burden analysts. Deep learning has been investigated as a way to learn complex patterns from traffic features, although practical deployment raises questions about dataset representativeness, computational cost, model explainability, robustness, privacy, and latency (Abu Al-Haija et al., 2022; Demertzis et al., 2021; Wang & Thing, 2023).

A critical distinction is that technical detection performance and users' or practitioners' trust in a detection system are related but different questions. A model may be technically capable yet difficult to justify to analysts, while a trusted system may still require independent performance validation. This article focuses on trust-related perceptions rather than claiming that a new deep-learning model was implemented or benchmarked.

1.1 Research objective and questions

The study examines the relationships between Privacy Issues, Threat Experience, Encryption Knowledge, and Detection Trust in the context of real-time threat detection for encrypted darknet traffic.

The research questions are: (1) How are privacy issues associated with trust in deep-learning-based threat detection? (2) How is prior threat experience associated with Detection Trust? (3) How is encryption knowledge associated with Detection Trust? (4) What practical and ethical requirements do interview participants identify for reliable real-time detection?

2. Related Work

Research on darknet traffic classification and encrypted malicious-traffic detection has explored machine-learning and deep-learning methods that use traffic characteristics rather than relying exclusively on payload inspection. Studies have considered darknet traffic detection, near-real-time encrypted traffic anomaly detection, feature mining, and hybrid or adaptive approaches (Abu Al-Haija et al., 2022; Demertzis et al., 2021; Ucci et al., 2021; Wang & Thing, 2023).

The literature discussed in the thesis also highlights recurring operational concerns: limited access to representative labelled datasets, class imbalance, distribution shifts, high computational demands, adversarial evasion, and limited interpretability. These concerns matter when systems are expected to operate on live traffic, where processing delays and incorrect alerts can affect operational decisions.

Privacy is a separate design requirement. Encrypted communication is not itself evidence of malicious intent, and monitoring may expose legitimate users to unnecessary scrutiny. A responsible approach should minimise data collection, restrict access and retention, document the purpose of monitoring, and provide human review for consequential decisions. Explainability and independent validation are therefore relevant not only to model development but also to the trust that practitioners place in automated alerts.

3. Methodology

3.1 Research design and participants

The thesis used a mixed-method design. The quantitative component analysed 151 questionnaire responses. The qualitative component comprised seven semi-structured interviews with participants whose backgrounds included cybersecurity, network security, digital forensics, research, and related information-technology areas. The two strands were used to examine statistical associations and to provide contextual accounts of practical concerns.

3.2 Measures and analysis

The questionnaire measured four constructs: Privacy Issues, Threat Experience, Encryption Knowledge, and Detection Trust. The thesis reports 20 questionnaire items across these constructs, measured using a five-point Likert scale. Internal consistency was assessed using Cronbach's alpha. Pearson correlation was used to examine pairwise associations, and multiple regression was used to assess the joint association of the three independent variables with Detection Trust. Interview material was analysed thematically.

3.3 Scope and interpretation

The survey and interviews measured perceptions and reported associations. They did not involve a controlled benchmark of a deployed deep-learning model, nor did they directly measure detection accuracy, false-positive rate, latency, throughput, or privacy-preserving technical performance. Accordingly, results are interpreted as evidence about Detection Trust and implementation expectations, not as proof of technical effectiveness or causality.

4. Results

4.1 Reliability

The 20 questionnaire items produced a reported Cronbach's alpha of 0.914, indicating high overall internal consistency for the instrument as a whole. The thesis notes that construct-specific reliability should be assessed separately before drawing stronger conclusions about each scale.

Measure	Reported result	Interpretation
Questionnaire items	20	Items represented four constructs
Valid questionnaire responses	151	Quantitative analysis sample
Cronbach's alpha	0.914	High overall internal consistency

4.2 Correlations with Detection Trust

All three independent variables were positively associated with Detection Trust. Encryption Knowledge had the strongest reported bivariate correlation, followed closely by Threat Experience. Privacy Issues also showed a moderate positive association. These correlations do not establish that any predictor causes greater trust.

Variable	Correlation with Detection Trust (r)	Reported significance
Privacy Issues	0.547	$p < .001$
Threat Experience	0.673	$p < .001$
Encryption Knowledge	0.682	$p < .001$

4.3 Multiple regression

The multiple regression model was statistically significant, $F(3,147) = 70.192$, $p < .001$. The model summary reported $R^2 = 0.589$ and adjusted $R^2 = 0.581$, indicating that the three predictors jointly accounted for 58.9% of the observed variance in Detection Trust within this sample. Encryption Knowledge had the largest reported standardised coefficient, followed by Threat Experience and Privacy Issues.

Predictor	Standardised coefficient (β)	Reported significance
Privacy Issues	0.187	$p = .004$
Threat Experience	0.341	$p < .001$
Encryption Knowledge	0.377	$p < .001$

The remaining 41.1% of variance was not explained by this model. The thesis identifies possible additional factors for future study, including perceived accuracy, transparency, prior experience with automated systems, organisational support, and tolerance for false-positive alerts. The coefficients should be checked against the original statistical output before journal submission because the thesis contains some inconsistencies in how coefficients are described in different passages.

4.4 Interview themes

Theme identified in the thesis	Summary of participants' concerns
Limited visibility into encrypted traffic	Payload encryption means detection often relies on indirect flow and metadata features.
Limitations of traditional tools	Known signatures and rules remain useful but may struggle with new behaviour and can generate excessive alerts.
Potential of deep learning and metadata	Participants saw potential in learning complex traffic patterns without directly reading message content.
Privacy and ethics	Monitoring should be proportionate and should not treat encryption or anonymity alone as evidence of wrongdoing.
Trust and explainability	Analysts need understandable reasons for alerts, realistic validation, and evidence of reliability.
Real-time implementation	Practical systems need low latency, scalability, continuous validation, and manageable computational requirements.

4.5 Integrated conceptual model

The study examined three predictors of Detection Trust. The figure below summarises the tested conceptual relationships; arrows represent associations evaluated in the study, not proven causal pathways.

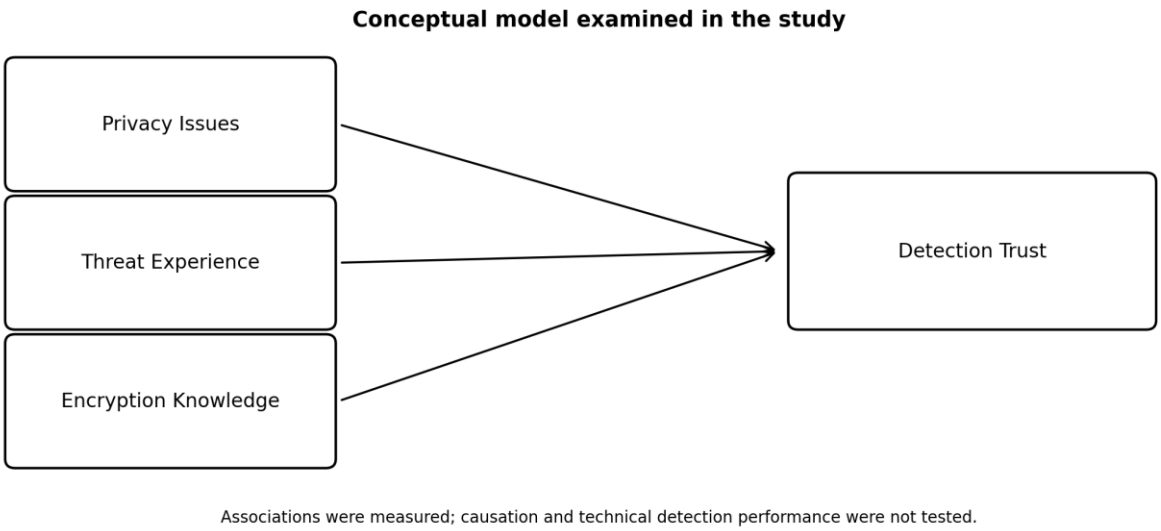


Figure 1. Conceptual relationships examined in the study. Source: Developed from the thesis constructs.

5. Discussion

The quantitative findings indicate that Detection Trust was associated with privacy-related perceptions, prior threat experience, and encryption knowledge. Encryption Knowledge showed the strongest bivariate relationship and the largest reported standardised coefficient in the regression model. One possible interpretation is that respondents who feel more informed about encryption may be better positioned to understand the constraints and potential of traffic-based detection. This interpretation remains tentative because the design is observational and the knowledge construct is self-reported.

Threat Experience was also positively associated with Detection Trust. Interview accounts suggest that practical familiarity with security alerts and limitations of existing tools may shape expectations of automated detection. However, the results do not establish that experience itself increases trust; other factors may influence both experience and trust.

The positive association between Privacy Issues and Detection Trust requires careful interpretation. The construct's item wording and coding determine what a higher score represents. It should not automatically be concluded that greater privacy concern causes greater trust. The thesis itself cautions that item wording and coding should be reviewed before making that inference.

The interviews complement the statistical results by identifying practical conditions under which a system might be considered credible: protection of legitimate encrypted communications, explainable alerts, independent testing on realistic traffic, low latency, scalability, and continuous validation. These are implementation requirements reported by participants, not measured properties of a tested detector.

5.1 Practical implications

First, system developers should separate threat classification from assumptions about user intent: encrypted or anonymous traffic should not, by itself, trigger a malicious classification. Second, monitoring should apply data minimisation, limited retention, access controls, and documented purposes. Third, deep-learning systems should be evaluated using representative datasets and metrics such as precision, recall, F1-score, false-positive rate, detection latency, throughput, and resource use. Fourth, explanations should provide analysts with interpretable evidence for alerts and retain human oversight for consequential actions. Finally, performance should be monitored after deployment to identify drift and emerging failure modes.

6. Limitations and Future Research

The study has several limitations. The quantitative sample comprised 151 respondents, and the qualitative component included seven interviews; the findings may not generalise to all cybersecurity settings. Questionnaire constructs were self-reported, and the design does not establish causal relationships. Although the thesis discusses deep-learning techniques, it does not report a direct experiment comparing detector architectures or provide benchmark results for accuracy, latency, false positives, or computational cost. The reported regression statistics and coefficient descriptions should be reconciled with the original statistical software output before submission.

Future work should validate the trust model in larger and more diverse samples, report construct-level reliability, and test whether trust changes after participants interact with a real detector. Technical studies should use reproducible datasets and clearly documented train/test splits, assess class imbalance and distribution shift, and report operational performance alongside privacy risks. Research should also examine whether explainability tools improve analysts' calibrated trust without introducing unacceptable latency.

7. Conclusion

This mixed-method study examined factors associated with trust in deep-learning-based real-time threat detection for encrypted darknet traffic. In a sample of 151 questionnaire respondents, Privacy Issues, Threat Experience, and Encryption Knowledge were positively correlated with Detection Trust. The three predictors jointly explained 58.9% of the variance reported by the thesis regression model. Seven interviews identified six recurring areas of concern, including limited payload visibility, conventional-tool limitations, the potential of metadata-based analysis, privacy and ethics, explainability, and real-time implementation.

The principal contribution is an account of trust-related perceptions and the operational safeguards participants considered important. The findings should not be presented as proof that a particular deep-learning model achieves high detection accuracy, because no such technical performance test was reported. Reliable deployment requires separate empirical validation, privacy safeguards, explainable alerts, and continuous monitoring.

References

1. Abu Al-Haija, Q., Krichen, M., & Abu Elhaija, W. (2022). Machine-learning-based darknet traffic detection system for IoT applications. Electronics, 11(4), 556. https://doi.org/10.3390/electronics11040556
2. Demertzis, K., Tsiknas, K., Takezis, D., Skianis, C., &Iliadis, L. (2021). Darknet traffic big-data analysis and network management for real-time automating of the malicious intent detection process by a weight agnostic neural networks framework. Electronics, 10(7), 781. https://doi.org/10.3390/electronics10070781
3. Ucci, D., Sobrero, F., Bisio, F., &Zorzino, M. (2021). Near-real-time anomaly detection in encrypted traffic using machine learning techniques. In 2021 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1–8). IEEE. https://ieeexplore.ieee.org/abstract/document/9659955/
4. Wang, Z., & Thing, V. L. (2023). Feature mining for encrypted malicious traffic detection with deep learning and other machine learning algorithms. Computers & Security, 128, 103143. https://doi.org/10.1016/j.cose.2023.103143
5. Yang, J., Liang, G., Li, B., Wen, G., & Gao, T. (2021). A deep-learning-and reinforcement-learning-based system for encrypted network malicious traffic detection. Electronics Letters, 57(9), 363–365. https://doi.org/10.1049/ell2.12125
6. Shinde, V., Singhal, K., Almogren, A., Dhanawat, V., Karande, V., & Rehman, A. U. (2024). Ensemble voting for enhanced robustness in darknet traffic detection. IEEE Access. https://ieeexplore.ieee.org/iel8/6287639/10380310/10740290.pdf
7. Villegas-Ch, W., Govea, J., Gutierrez, R., Navarro, A. M., & Mera-Navarrete, A. (2024). Effectiveness of an adaptive deep learning-based intrusion detection system. IEEE Access. https://ieeexplore.ieee.org/iel8/6287639/6514899/10778531.pdf