TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 24, No. 4, August 2026, pp. 1241~1252
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v24i4.27791

Acoustic and vibration side channel analysis on post-quantum cryptography using image-based deep learning

Abdul Haris Muhammad, Gamaria Mandar, Adelina Ibrahim
Informatics Engineering Study Program, Muhammadiyah University of North Maluku, Ternate, Indonesia

Article Info

Article history:

Received Jan 10, 2026
Revised Apr 6, 2026
Accepted May 25, 2026

Keywords:

Acoustic leakage
Deep learning
Post-quantum cryptogrphy
Side-channel attack
Vibration analysis

ABSTRACT

Post-quantum cryptography (PQC) is designed to resist quantum-era attacks; however, practical implementations remain vulnerable to physical side-channel leakage. This work proposes an image-based acoustic–vibration side-channel analysis framework to assess non-invasive leakage in PQC systems. Acoustic and vibration signals from secret-dependent executions are modeled and transformed into time–frequency spectrograms using short-time fourier transform (STFT). The dataset comprises 1,545 samples (1,236 training and 309 testing), acquired at 16 kHz and segmented into 2.5-second windows. Leakage classification is performed using convolutional neural networks (CNNs) and vision transformers (ViTs) under single-modality and multimodal fusion settings. Results show that acoustic signals yield strong leakage, achieving up to 100% accuracy with CNN, while vibration signals reach up to 98.75%. Multimodal fusion improves training stability and overall performance, and ViT models demonstrate better generalization across modalities. These findings confirm that multimodal spectrogram-based deep learning is effective for PQC side-channel analysis and underscore the need for rigorous physical security evaluation in real-world PQC implementations.

Corresponding Author:

Abdul Haris Muhammad
Informatics Engineering Study Program, Muhammadiyah University of North Maluku
KH Ahmad Dahlan Street No 100, Sasa, Ternate City, North Maluku, Indonesia
Email: agry.arisandi@gmail.com

1. INTRODUCTION

Quantum computing exploits principles of quantum mechanics to perform computations beyond classical capabilities by utilizing qubits that exist in superposition states. This enables efficient solutions to problems such as large integer factorization, which are infeasible for classical systems. For instance, Shor's algorithm can break widely used cryptographic schemes such as Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (ECC), posing significant risks to data security [1], [2]. In addition, quantum data processing often relies on encoding techniques such as amplitude and angle encoding, which may not preserve information in a lossless manner, particularly for image-based processing tasks [3], [4].

To address these threats, post-quantum cryptography (PQC) has been developed to ensure security against both classical and quantum attacks. PQC schemes are based on alternative hard problems, including lattice-based, code-based, hash-based, and multivariate cryptography, which are currently considered resistant to quantum algorithms [5]-[7]. However, the security of cryptographic systems depends not only on their mathematical strength but also on their implementation. In practice, cryptographic operations often produce unintended physical leakage, known as side-channel leakage, which can be exploited to recover sensitive information such as secret keys [8]-[13].

Among the various types of side channels, acoustic and mechanical vibration-based leakages remain significantly less explored compared to power consumption and electromagnetic emissions. Mechanical vibrations and acoustic signals can naturally arise from processor activity, electronic components, and the mechanical structure of computing devices during the execution of cryptographic algorithms. Furthermore, the widespread availability of microphones and accelerometers, including those embedded in consumer-grade devices, enables the non-invasive acquisition of acoustic and vibration signals, thereby increasing potential security risks [14], [15]. Among various side channels, acoustic and vibration-based leakage remains underexplored compared to power and electromagnetic channels. These signals naturally arise from device operations and can be captured non-invasively using common sensors such as microphones and accelerometers, increasing potential security risks [14], [15]. Existing studies primarily focus on classical cryptography and rely on manual or one-dimensional feature extraction methods, which are limited in capturing complex and noisy leakage patterns [16]-[20].

Despite extensive research on side-channel attacks targeting classical cryptographic implementations, studies focusing specifically on acoustic and vibration-based leakage in PQC remain very limited. Existing side-channel analyses predominantly investigate power or electromagnetic leakage and are largely centered on classical cryptosystems, while acoustic and vibration channels are often overlooked, particularly in the context of PQC implementations. Moreover, most prior works rely on single-modality analysis and manual or one-dimensional feature extraction techniques, which are insufficient for modeling the complex, non-linear leakage patterns produced by modern cryptographic execution. This reveals a critical research gap in the lack of comprehensive multimodal side-channel analysis frameworks capable of capturing correlated leakage behavior across multiple physical domains in PQC systems.

This limitation leads to a significant problem: current side-channel analysis methods and security evaluation frameworks are not adequately designed to detect, model, or mitigate multimodal acoustic and vibration leakage in PQC implementations. As a result, the true extent of information leakage in real-world environments remains poorly understood, potentially leaving PQC systems vulnerable to non-invasive and covert attacks.

To address this gap, this study introduces a multimodal, image-based side-channel analysis framework that jointly exploits acoustic and vibration leakage in PQC implementations. By transforming physical leakage signals into spectrogram representations, the proposed approach leverages convolutional neural networks (CNNs) and vision transformers (ViTs) to capture both local and global leakage characteristics across modalities. To the best of our knowledge, this work is among the first to systematically investigate multimodal acoustic–vibration spectrogram fusion using deep learning for side-channel analysis of PQC implementations.

In light of the aforementioned challenges, this research proposes a novel approach for analyzing acoustic and vibration side-channel leakage in PQC implementations using a multimodal, image-based deep learning framework. The primary objective of this study is to develop a side-channel analysis model capable of capturing the relationship between secret-dependent PQC execution and the resulting physical leakage signals. Furthermore, this research aims to evaluate the extent to which sensitive information can be inferred from acoustic and vibration emissions and to assess the effectiveness of multimodal fusion by integrating both modalities and comparing the results with single-modality analysis. To achieve this, acoustic and vibration signals are transformed into image-based representations through spectrogram encoding, enabling the application of CNNs and ViTs for feature extraction and leakage inference. By eliminating the reliance on manual feature engineering, the proposed image-based approach facilitates the learning of complex and non-linear leakage patterns that are difficult to model using conventional signal processing techniques, thereby providing a more comprehensive physical security evaluation of PQC implementations.

2. RELATED WORKS

2.1. PQC

PQC is a field of cryptography that focuses on designing cryptographic algorithms that are resistant to and secure against quantum-computer attacks. Unlike conventional cryptographic schemes, which generally rely on mathematical problems such as integer factorization and discrete logarithms, PQC algorithms are designed around problems believed to be difficult to solve even with quantum computers. Therefore, PQC is considered a long-term solution for maintaining information system security in the future [21].

2.2. PQC framework

Various approaches have been developed for PQC, which can be broadly classified into five categories. First, hash-based cryptography focuses on digital signatures secured by hash functions, requiring fewer assumptions compared to number-theoretic schemes such as RSA and dynamic spectrum access (DSA) [22].

Second, code-based cryptography relies on the hardness of decoding problems, such as syndrome decoding and learning parity with noise, with the McEliece scheme being a prominent example and National Institute of Standards and Technology (NIST) finalist [23]-[25]. Third, multivariate cryptography is based on solving systems of multivariate polynomial equations, with schemes such as unbalanced oil and vinegar (UOV) and rainbow widely used for digital signatures [26], [27].

Fourth, lattice-based cryptography has become the most dominant PQC approach due to its strong security foundations on problems such as shortest vector problem (SVP) and ring learning with errors (RLWE), while also enabling advanced primitives like homomorphic encryption; examples include NewHope and bimodal lattice signature scheme (BLISS) [28]-[30]. Finally, isogeny-based cryptography utilizes mappings between supersingular elliptic curves, offering compact key sizes but high computational complexity, as seen in supersingular isogeny Diffie–Hellman (SIDH) and supersingular isogeny key encapsulation (SIKE) [31]-[34]. As illustrated in Figure 1, side-channel attacks can be categorized into power, timing, and physical leakage-based attacks, including acoustic side-channel attacks (ASCAs). Unlike invasive methods, ASCAs exploit sound emissions without requiring physical modification of the target system, making them difficult to detect [35]. Consequently, cryptographic implementations that are secure against mathematical attacks may still leak sensitive information through acoustic channels, posing a significant real-world threat [36].

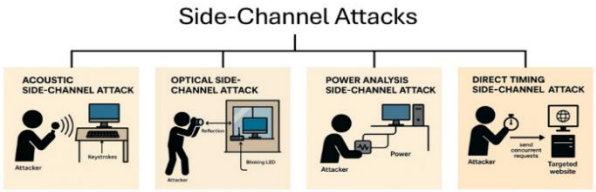


Figure 1. Types of ASCAs [37]

ASCAs have emerged as a significant threat to information security; however, a unified framework for classifying attack modalities, evaluating mitigation strategies, and identifying emerging vectors remains lacking [37]. Recent studies have explored advanced analytical approaches, including reconstructing discriminative features from far-field electromagnetic emissions, demonstrating that sensitive information can be extracted even in noisy and non-invasive settings [38]. In addition, deep learning-based fusion strategies have improved profiling attacks by integrating features from multiple CNNs, enhancing robustness and generalization [39]. Nevertheless, most existing approaches rely on single-modality inputs or one-dimensional representations, limiting their ability to capture complex multimodal leakage patterns.

Deep learning-based side-channel analysis has gradually replaced traditional signal processing methods. Evaluations on benchmark datasets such as ASCAD highlight the importance of CNN architecture design and hyperparameter configuration in determining attack performance [40], [41]. To address this, recent studies have proposed automated optimization strategies, including model fusion and adaptive learning techniques, to improve robustness and generalization [42], [43].

Ensemble learning approaches further enhance performance by leveraging model diversity, while shift-invariant temporal networks address misalignment issues in side-channel traces [44], [45]. Moreover, automated hyperparameter optimization using techniques such as Bayesian optimization and reinforcement learning has been investigated to reduce manual tuning and improve model stability [46]-[48].

Generative learning approaches, such as conditional generative adversarial networks (cGANs), have also been explored to reduce dependency on large profiling datasets by synthesizing side-channel traces. However, such generative approaches often incur high computational costs and long training times due to model complexity, which poses significant challenges for deployment in resource-constrained environments [49]. Despite these advances, most deep learning-based approaches still rely heavily on large, high-quality datasets, which remain difficult to obtain in practical scenarios.

3. METHOD

This study investigates information leakage in PQC implementations through acoustic and vibration-based side channels using an image-based deep learning framework. Acoustic and vibration signals were collected during secret-dependent cryptographic executions using non-invasive acquisition techniques, as commonly adopted in recent studies [50], [51].

The dataset comprises four classes representing different cryptographic operations, with a total of 2000 samples. The original dataset contains 600 samples, which were expanded through data augmentation techniques, including noise injection, time shifting, and frequency masking, to enhance robustness and generalization. The dataset was split into training, validation, and testing sets with a ratio of 70%:10%:20%. The raw signals were transformed into time–frequency representations using spectrogram encoding, which effectively preserves temporal and spectral characteristics for side-channel analysis [52], [53]. CNNs were employed for local feature extraction, while ViTs were utilized to capture global dependencies through self-attention mechanisms [54]-[56]. Furthermore, a multimodal fusion strategy was implemented by integrating acoustic and vibration modalities to improve robustness and generalization [57]-[59].

For evaluation, CNN was used as a baseline model, while ViT served as a comparative architecture to assess global feature learning capability. Three input configurations (acoustic, vibration, and multimodal fusion) were systematically evaluated. Traditional machine learning models were not considered, as this study focuses on deep learning approaches for modeling complex leakage patterns. Figure 2 illustrates the overall research framework, including data acquisition, preprocessing, spectrogram transformation, multimodal fusion, and model evaluation.

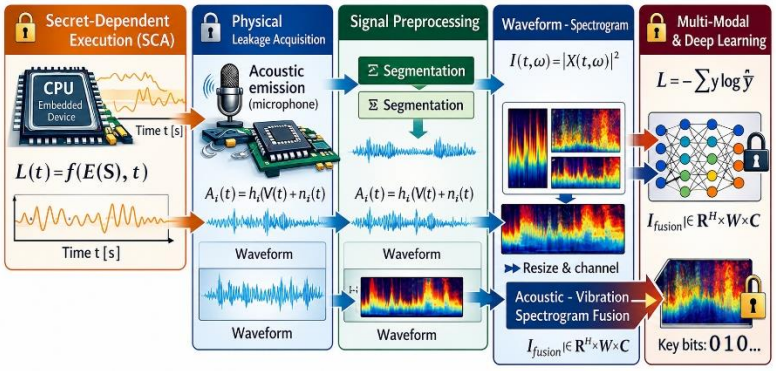


Figure 2. Acoustic and vibration side channel analysis research method

The proposed framework consists of six stages for analyzing side-channel leakage in PQC implementations. In the first stage, secret-dependent execution is modeled, where the internal execution path of a cryptographic algorithm depends on the secret value S. The leakage source is defined as:

$$L(t) = f(E(S), t) \tag{1}$$

where $E(S)$represents the execution path and $L(t)$denotes time-varying computational activity. This activity produces observable physical leakage despite the mathematical security of PQC.

The second stage involves non-invasive physical leakage acquisition using acoustic (microphone) and vibration (accelerometer) sensors. The observed signal is modeled as:

$$A_a(t) = h_a(V(t)) + n_a(t) \tag{2}$$

where $V(t)$is internal activity and $n_a(t)$ is environmental noise. Sensors are placed near the device without hardware modification.

In the third stage, preprocessing is applied, including normalization, segmentation, and temporal alignment. Signals are recorded at 16 kHz with 2.5-second duration per sample. The fourth stage transforms signals into spectrograms using short-time fourier transform (STFT):

$$I(t, w) = |X(t, w)|^2 \tag{3}$$

with a window size of 1024 samples and 50% overlap. Spectrograms preserve temporal-spectral characteristics for image-based analysis. The fifth stage performs multimodal fusion at the image level:

$$I_{fusion} \in \mathbb{R}^{H\ x\ W\ x\ C} \tag{4}$$

Combining acoustic and vibration information to capture cross-modal correlations. Finally, deep learning models (CNN and ViT) are used for classification. The training objective is defined as:

$$L = -\sum y \log \hat{y} \quad (5)$$

where y is the true label and $\hat{y}$ is the prediction. Early stopping and learning rate scheduling are applied to ensure stable training.

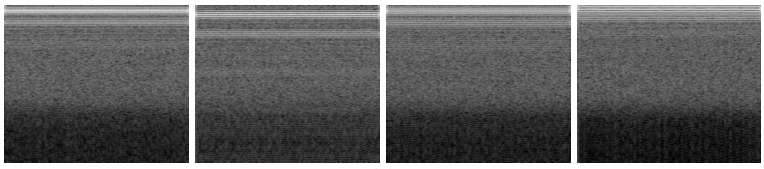
This framework demonstrates that sensitive information can be inferred from non-invasive leakage in PQC implementations. Although the dataset is limited and partially augmented, this study focuses on comparative analysis across modalities and architectures under controlled conditions. This formulation ensures reproducibility and provides a clear mapping between physical leakage modeling and deep learning-based inference.

4. RESULTS AND DISCUSSION

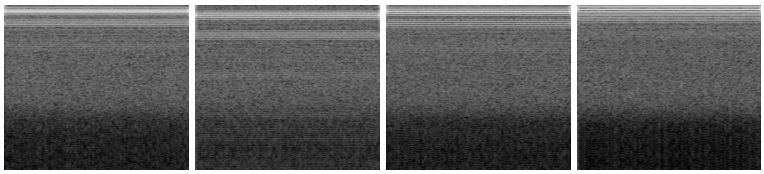
This section presents the experimental results and discussion of the proposed image-based multimodal side-channel analysis for PQC. The evaluation compares three scenarios acoustic, vibration, and acoustic–vibration fusion using CNNs and ViTs. The experiments aim to assess: (i) the capability of each modality to represent information leakage, (ii) the effectiveness of multimodal fusion in improving inference performance, and (iii) the impact of data augmentation on model stability and generalization. Results are presented through spectrogram visualizations, learning curves, confusion matrices, and quantitative metrics.

The dataset was constructed from physical leakage signals generated during PQC execution, consisting of acoustic signals (microphone) and vibration signals (sensor-based). To address limited profiling traces, synthetic data augmentation was applied, resulting in 300-500 samples per class. Signals were recorded at a sampling rate of 16 kHz with a duration of 2.5 seconds, then transformed into fixed-size spectrograms and split into training, validation, and testing sets with a ratio of 70%:10%:20%.

Figure 3 shows representative spectrogram visualizations for acoustic, vibration, and fused modalities across different secret classes, serving as inputs for the proposed deep learning models. Figures 3(a) and (b) show the spectrogram representation of the acoustic side channel signal corresponding to two different executions that depend on the secret. The acoustic spectrogram shows prominent horizontal frequency bands and energy concentration patterns that vary according to the secret value. This difference indicates that acoustic emissions capture execution-dependent characteristics of PQC calculations, making them a strong source of side-channel leakage.



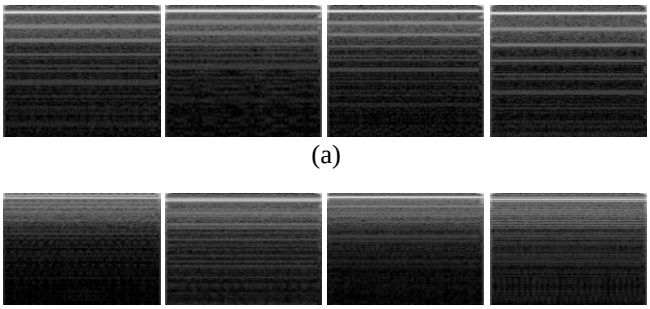
(a)



(b)

Figure 3. The spectrogram representation of acoustic side-channel leakage: (a) secret 0 and (b) secret 1

Figures 4(a) and (b) illustrate vibration-based spectrograms derived from mechanical responses during cryptographic execution. Compared to acoustic signals, vibration spectrograms exhibit a smoother, more dispersed energy distribution, and although leakage patterns are less visually apparent, different structural variations can still be observed across secret classes, indicating that vibration signals provide complementary but weaker side-channel information.

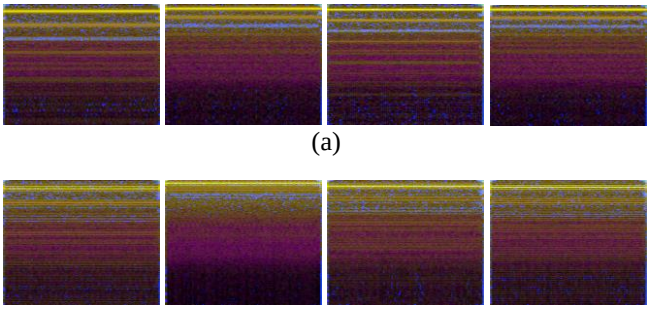


(a)

(b)

Figure 4. The spectrogram representation of vibration-based side-channel leakage: (a) secret 0 and (b) secret 1

Figures 5(a) and (b) show combined spectrograms. These images are created by combining acoustic and vibration data into a single multi-channel format. This combined image highlights the shared and different features of the two types of physical leakage. This integrated approach helps clarify the patterns of secret-dependent execution, providing more input data for deep learning models.



(a)

(b)

Figure 5. The multimodal fusion spectrogram combining acoustic and vibration information: (a) secret 0 and (b) secret 1

This spectrogram and fusion image are directly related to the image processing and multi-modal fusion stages illustrated in the system architecture proposed in Figure 2, which serves as fundamental input for a CNN and ViT-based side channel analysis. Figure 6 illustrates the training and validation learning curves of CNN and ViTs models across acoustic, vibration, and multimodal fusion scenarios.

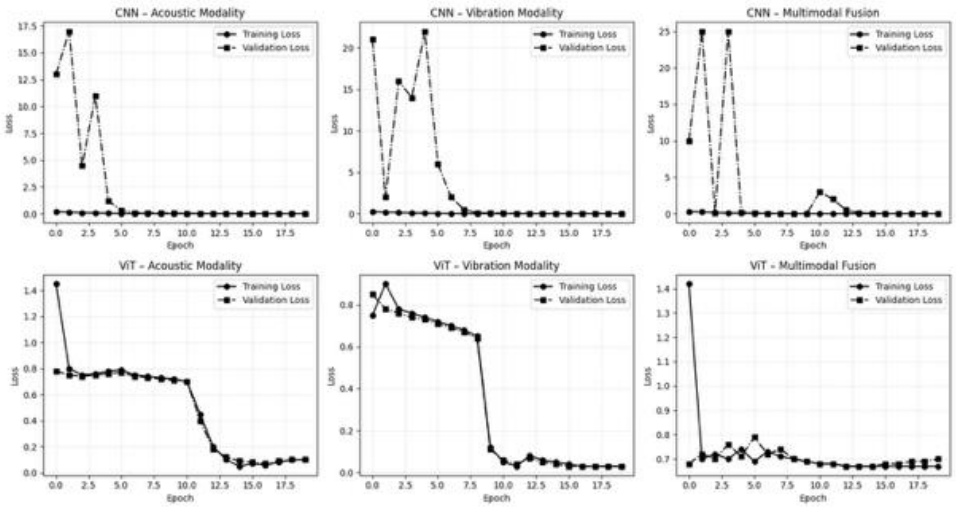
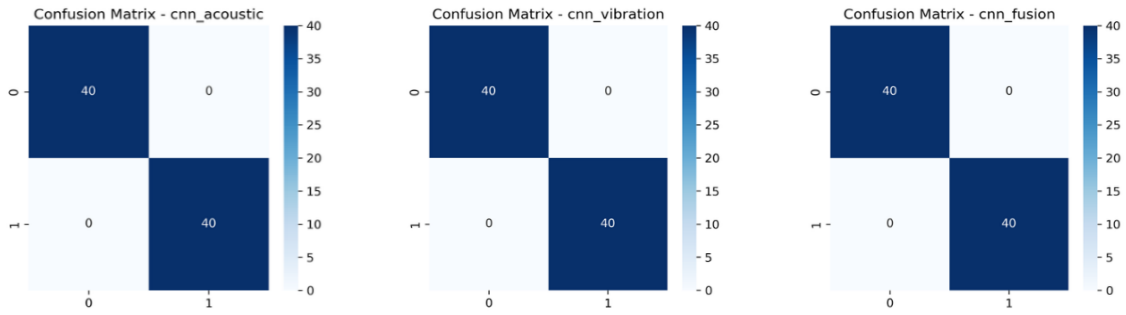


Figure 6. Learning curves for CNN, ViT, and multi-modal fusion

Figure 6 presents the training and validation loss curves of CNN and ViT models across three scenarios: acoustic, vibration, and multimodal fusion. CNN models show rapid convergence with near-zero training loss within a few epochs across all modalities, indicating strong capability in capturing local leakage patterns. However, this behavior also suggests potential overfitting, particularly in the acoustic modality where structured leakage is easier to learn. The vibration modality exhibits slightly higher instability, reflecting its lower signal-to-noise ratio and more complex leakage characteristics. In the fusion scenario, CNN convergence remains fast, but the learning pattern indicates limited exploitation of cross-modal dependencies.

In contrast, ViT models demonstrate more gradual and stable convergence with closely aligned training and validation losses, indicating better generalization. This advantage is especially evident in the vibration modality, where ViT effectively captures dispersed and less structured leakage patterns. In the multimodal fusion setting, ViT achieves the most stable learning behavior, suggesting its effectiveness in integrating complementary information across modalities. Figure 7 presents the confusion matrices of CNN-based classification results for acoustic (Figure 7(a)), vibration (Figure 7(b)), and multimodal fusion side-channel inputs (Figure 7(c)).



(a) (b) (c)

Figure 7. Confusion matrices of CNN-based classification results: (a) acoustic, (b) vibration, and (c) multimodal fusion inputs

Figure 7 shows the confusion matrices of CNN-based models across acoustic, vibration, and multimodal fusion scenarios. All models achieve perfect classification accuracy, with no misclassification observed. This indicates that both acoustic and vibration spectrograms contain strong discriminative leakage patterns during PQC execution.

The acoustic modality demonstrates highly structured leakage, enabling effective extraction of local features. Similarly, despite lower signal-to-noise characteristics, vibration signals still provide sufficient information for accurate classification. In the multimodal fusion scenario, the CNN model maintains perfect performance.

However, the consistent 100% accuracy across all modalities suggests that the dataset may be relatively simple or that the model may have overfitted. Consequently, the advantage of multimodal fusion over single-modality inputs cannot be conclusively determined based solely on accuracy. These results confirm the effectiveness of CNN in capturing side-channel leakage patterns, while also highlighting the need for further evaluation using more complex datasets, noise conditions, or cross-validation strategies to assess generalization performance. Figure 8 presents the confusion matrices of ViT-based models for comparison.

In contrast to CNN results, the acoustic-based ViT model in Figure 8(a) shows minor misclassification, with one sample incorrectly classified. Although overall performance remains high, this indicates that ViT captures more distributed and global leakage representations through self-attention, rather than relying on dominant local features.

For the vibration modality (Figure 8(b)), ViT also achieves high performance with minimal errors. Combined with the learning curve analysis, this suggests improved generalization capability, particularly for weaker and more spatially distributed leakage patterns. The ability of ViT to model long-range dependencies enables more effective extraction of subtle features compared to CNN.

However, in the multimodal fusion scenario (Figure 8(c)), a performance decrease is observed compared to single-modality inputs. This indicates that the fusion strategy used in this study does not fully exploit cross-modal relationships within the ViT architecture. The result suggests that more advanced fusion mechanisms, larger datasets, or better feature alignment are required.

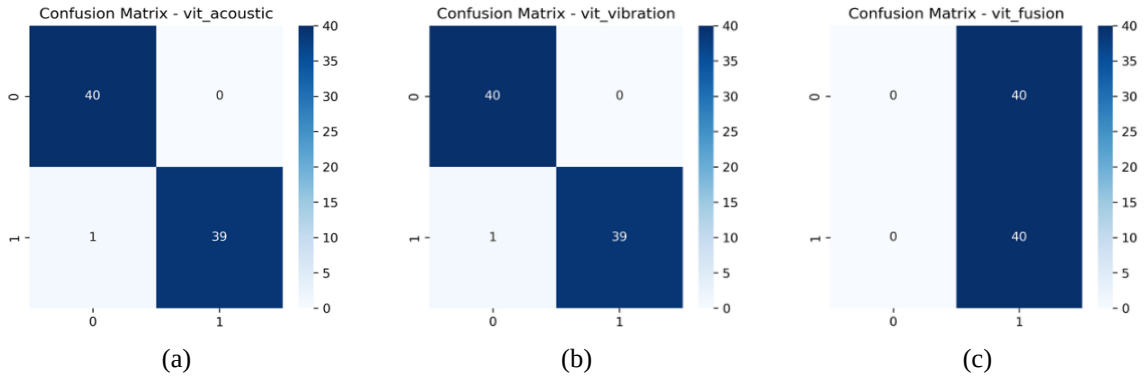


Figure 8. Confusion matrices of ViT-based classification results: (a) acoustic, (b) vibration, and (c) multimodal fusion inputs

Overall, ViT demonstrates strong generalization for single-modality inputs, but its effectiveness in multimodal settings depends on the design of the fusion strategy and data scale. Table 1 presents a quantitative comparison of performance in terms of accuracy, precision, recall, and F1-score across all models and modalities.

Table 1. Classification performance of CNN and ViT models for different side-channel modalities

Models	Accuracy	Precision	Recall	F1-score
cnn_acoustic	1.0	1.0	1.0	1.0
cnn_vibration	1.0	1.0	1.0	1.0
cnn_fusion	1.0	1.0	1.0	1.0
vit_acoustic	0.9875	0.9878048780487805	0.9875	0.9874980465697765
vit_vibration	0.9875	0.9878048780487805	0.9875	0.9874980465697765
vit_fusion	0.5	0.25	0.5	0.3333333333333333

From Table 1, classification performance is influenced by both modality and model architecture. CNN models achieve near-perfect results across all modalities (all metrics = 1.0), indicating a strong capability to capture structured leakage patterns from spectrograms. In contrast, ViT models show slightly lower performance for single modalities, with 98.75% accuracy for both acoustic and vibration inputs, suggesting that their reliance on global representations may be less effective than CNNs in exploiting highly localized leakage features.

A significant performance drop is observed in the multimodal ViT configuration, where accuracy decreases to 50% and the F1-score to 0.33, indicating that the simple fusion strategy is not well aligned with transformer-based architectures and highlighting the model's sensitivity to feature alignment and data scale. These findings should be interpreted within the context of controlled laboratory conditions rather than as guarantees of real-world performance, as the practical feasibility of exploiting leakage also depends on factors such as environmental noise, device variability, and implementation differences.

Consistent with prior studies [16]-[18], this work confirms the presence of physical leakage in cryptographic systems. However, unlike previous single-modality approaches, this study introduces a multimodal acoustic–vibration framework using image-based deep learning to capture more complex leakage patterns. From a security perspective, the findings highlight the need for countermeasures such as acoustic shielding, noise injection, randomized execution, and hardware-level protection.

Despite promising results, limitations remain, including limited dataset size, reliance on synthetic augmentation, controlled experimental conditions, and a simple fusion strategy. Future work should focus on larger datasets, real-world acquisition settings, and advanced fusion mechanisms to improve robustness and generalization.

5. CONCLUSION

This study demonstrates that PQC implementations remain susceptible to non-invasive physical side-channel leakage, despite their theoretical resistance to quantum-based cryptanalysis. The experimental results indicate that acoustic emissions generally exhibit stronger and more structured leakage characteristics

than mechanical vibrations, while the integration of multimodal acoustic–vibration representations consistently enhances learning stability and classification performance. The comparative evaluation of deep learning architectures further reveals that CNNs achieve faster convergence but are more sensitive to noise and overfitting, whereas ViT models provide improved robustness and generalization when handling complex and non-linear leakage patterns.

These findings highlight that combining acoustic and vibration modalities with appropriate image-based deep learning architectures constitutes an effective approach for side-channel analysis in post-quantum cryptography. To the best of our knowledge, this work represents one of the first systematic investigations of multimodal acoustic–vibration spectrogram fusion for physical leakage analysis in PQC implementations. The results emphasize the importance of evaluating physical implementation security alongside mathematical resistance, particularly for cryptographic systems deployed in practical environments.

Future research will extend this work toward larger and more diverse datasets, real hardware-based PQC implementations, and robustness evaluation under noisy and heterogeneous operating conditions, including remote attack scenarios. Additional research directions include the exploration of advanced fusion strategies such as attention-based mechanisms, adversarial obfuscation defenses, and explainable AI techniques to enhance both the interpretability and resilience of side-channel analysis frameworks. In this context, the proposed framework is particularly relevant for evaluating the physical security of PQC implementations in emerging Internet of Things (IoT) and embedded systems.

ACKNOWLEDGMENTS

The author would like to thank the Informatics Engineering Study Program, Muhammadiyah University of North Maluku for their assistance in this research.

FUNDING INFORMATION

The author would like to express his gratitude to the Informatics Engineering Study Program, Faculty of Engineering, Muhammadiyah University of North Maluku, Ternate.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Abdul Haris Muhammad	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
Gamaria Mandar	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓
Adelina Ibrahim				✓	✓	✓				✓		✓		✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no conflict of interest.

DATA AVAILABILITY

The datasets generated and/or analyzed during the current study are available from the corresponding author upon reasonable request.

REFERENCES

[1] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang, "A Survey of Post-Quantum Cryptography: Start of a New Race," *Cryptography*, vol. 7, no. 3, p. 40, Aug. 2023, doi: 10.3390/cryptography7030040.
[2] D. Ukpabi *et al.*, "Framework for understanding quantum computing use cases from a multidisciplinary perspective and future

research directions," *Futures*, vol. 154, p. 103277, Dec. 2023, doi: 10.1016/j.futures.2023.103277.
[3] J. Zhang et al., "Design and implementation of run-length encoding on quantum computers for resource-efficient data representation," *Applied Soft Computing*, vol. 187, p. 114273, Feb. 2026, doi: 10.1016/j.asoc.2025.114273.
[4] C. Hao, Q. Ma, Y. Chen, H. Zhang, and D. Qu, "Quantum autoencoder implementation of high-dimensional steganographic encoding for arbitrary quantum states," *Journal of King Saud University Computer and Information Sciences*, vol. 37, no. 8, Oct. 2025, doi: 10.1007/s44443-025-00274-1.
[5] S. Mandrà, H. Munoz-Bauza, G. Mossi, and E. G. Rieffel, "Generating hard Ising instances with planted solutions using post-quantum cryptographic protocols," *Future Generation Computer Systems*, vol. 166, p. 107721, May 2025, doi: 10.1016/j.future.2025.107721.
[6] Y. Kim *et al.*, "Evidence for the utility of quantum computing before fault tolerance," *Nature*, vol. 618, no. 7965, pp. 500–505, Jun. 2023, doi: 10.1038/s41586-023-06096-3.
[7] S. Ahmadunnisa and S. E. Mathe, "A comprehensive review on hardware implementations of lattice-based cryptographic schemes," *Journal of Systems Architecture*, vol. 167, p. 103486, Oct. 2025, doi: 10.1016/j.sysarc.2025.103486.
[8] M. Bandaru, S. E. Mathe, and C. Wattanapanich, "Evaluation of hardware and software implementations for NIST finalist and fourth-round post-quantum cryptography KEMs," *Computers and Electrical Engineering*, vol. 120, p. 109826, Dec. 2024, doi: 10.1016/j.compeleceng.2024.109826.
[9] E. W. Abood, A. A. Yassin, Z. A. Abduljabbar, V. O. Nyangaresi, and A. H. Ali, "Provably lightweight and secure IoHT scheme with post-quantum cryptography and fog computing: A comprehensive scheme for healthcare system," *MethodsX*, vol. 15, p. 103631, Dec. 2025, doi: 10.1016/j.mex.2025.103631.
[10] T.-T. Tsai and J.-H. Yang, "Leakage-resilient certificateless public key encryption with equality test resistant to side-channel attacks," *Computer Networks*, vol. 270, p. 111485, Oct. 2025, doi: 10.1016/j.comnet.2025.111485.
[11] J. Liao, H. Wang, J. Wang, and Y. Tang, "Switch-T: A novel multi-task deep-learning network for cross-device side-channel attack," *Journal of Information Security and Applications*, vol. 93, p. 104146, Sep. 2025, doi: 10.1016/j.jisa.2025.104146.
[12] V. S. Bokharaie and A. Jahanian, "Power side-channel leakage assessment and locating the exact sources of leakage at the early stages of ASIC design process," *The Journal of Supercomputing*, vol. 78, no. 2, pp. 2219–2244, Jun. 2021, doi: 10.1007/s11227-021-03927-w.
[13] J. Xi and C. Fan, "Multi-byte side-channel attacks on chaotic block cipher: Autoencoder-based feature selection and CNN-Transformer collaborative attack framework," *Chaos, Solitons & Fractals*, vol. 200, p. 117097, Nov. 2025, doi: 10.1016/j.chaos.2025.117097.
[14] Sriramudu, V. Nalla, D. Narendar, and G. Padmavathi, "Model for capturing noise free traces for Side Channel Power Cryptanalysis based on SAKURA-G FPGA and Case study of AES," *2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC)*, pp. 1–7, Dec. 28, 2022. doi: 10.1109/icmacc54824.2022.10093672.
[15] Z. Huang, H. Wang, B. Cao, D. He, and J. Wang, "A comprehensive side-channel leakage assessment of CRYSTALS-Kyber in IIoT," *Internet of Things*, vol. 27, p. 101331, Oct. 2024, doi: 10.1016/j.iot.2024.101331.
[16] K. Yang, Y. Zhang, T. Li, and L. Sun, "ASIDS: Acoustic side-channel based intrusion detection system for industrial robotic arms," *Computers & Security*, vol. 157, p. 104586, Oct. 2025, doi: 10.1016/j.cose.2025.104586.
[17] Aakash, V. K. Pandey, S. Prakash, S. Singh, T. Yang, and R. S. Rathore, "An Efficient Approach for Side Channel Attack in Cloud Computing," *Procedia Computer Science*, vol. 258, pp. 1404–1413, 2025, doi: 10.1016/j.procs.2025.04.373.
[18] S. Alabdulwahab, M. Cheong, A. Seo, Y.-T. Kim, and Y. Son, "Enhancing deep learning-based side-channel analysis using feature engineering in a fully simulated IoT system," *Expert Systems with Applications*, vol. 266, p. 126079, Mar. 2025, doi: 10.1016/j.eswa.2024.126079.
[19] M. Mushtaq, M. A. Mukhtar, V. Lapotre, M. K. Bhatti, and G. Gogniat, "Winter is here! A decade of cache-based side-channel attacks, detection & mitigation for RSA," *Information Systems*, vol. 92, p. 101524, Sep. 2020, doi: 10.1016/j.is.2020.101524.
[20] V. S. Bokharaie and A. Jahanian, "Side-channel leakage assessment metrics and methodologies at design cycle: A case study for a cryptosystem," *Journal of Information Security and Applications*, vol. 54, p. 102561, Oct. 2020, doi: 10.1016/j.jisa.2020.102561.
[21] S. Hoque, A. Aydeger, and E. Zeydan, "Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design," *Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems*, pp. 9–16, Jun. 03, 2024. doi: 10.1145/3659997.3660033.
[22] C. Balamurugan, K. Singh, G. Ganesan, and M. Rajarajan, "Post-Quantum and Code-Based Cryptography—Some Prospective Research Directions," *Cryptography*, vol. 5, no. 4, p. 38, Dec. 2021, doi: 10.3390/cryptography5040038.
[23] S. Kumari, "Next-Gen IoT Security using Polar Codes-based Cryptography for malware defence through quantum self-attention neural network," *Knowledge-Based Systems*, vol. 321, p. 113716, Jun. 2025, doi: 10.1016/j.knosys.2025.113716.
[24] A. Saravanaselvan and B. Paramasivan, "An one-time pad cryptographic algorithm with Huffman Source Coding based energy aware sensor node design," *Sustainable Computing: Informatics and Systems*, vol. 44, p. 101048, Dec. 2024, doi: 10.1016/j.suscom.2024.101048.
[25] Z. Fu, L. Fang, H. Huang, and B. Yu, "Distributed three-level QR codes based on visual cryptography scheme," *Journal of Visual Communication and Image Representation*, vol. 87, p. 103567, Aug. 2022, doi: 10.1016/j.jvcir.2022.103567.
[26] D. Mishra, K. Namdeo, and N. Srivastava, "The rise and resilience of multivariate cryptography: Advances, pitfalls, and promising pathways," *Computer Science Review*, vol. 59, p. 100860, Feb. 2026, doi: 10.1016/j.cosrev.2025.100860.
[27] N. Kundu, S. K. Debnath, and D. Mishra, "A secure and efficient group signature scheme based on multivariate public key cryptography," *Journal of Information Security and Applications*, vol. 58, p. 102776, May 2021, doi: 10.1016/j.jisa.2021.102776.
[28] R. Iyswarya and R. Anitha, "Secure data storage in multi-cloud environments using lattice-based saber with Diffie-Hellman cryptography and authentication based on PUF-ECC," *Data & Knowledge Engineering*, vol. 161, p. 102512, Jan. 2026, doi: 10.1016/j.datak.2025.102512.
[29] M. G. A. Malik, M. Hussain, and Z. Bashir, "Efficient lattice-based Mordell elliptic curve S-box for secure lightweight cryptography," *Integration*, vol. 105, p. 102505, Nov. 2025, doi: 10.1016/j.vlsi.2025.102505.
[30] Q. I. M. Hussain and V. Kale, "Mobile node authentication with risk-based modified lattice cryptography enabled adaptive multifactor authentication for secure data transmission," *Computers and Electrical Engineering*, vol. 124, p. 110272, May 2025, doi: 10.1016/j.compeleceng.2025.110272.
[31] Y. Huang, Y. Jin, Z. Hu, and F. Zhang, "Optimizing the evaluation of ℓ-isogenous curve for isogeny-based cryptography," *Information Processing Letters*, vol. 178, p. 106301, Nov. 2022, doi: 10.1016/j.ipl.2022.106301.
[32] P. Dartois, "Fast computation of 2-isogenies in dimension 4 and cryptographic applications," *Journal of Algebra*, vol. 683, pp. 449–514, Dec. 2025, doi: 10.1016/j.jalgebra.2025.06.033.

[33] C. Chen, F. Zhang, and C. Zhao, "Isogeny computation on Kummer lines and applications," *Journal of Information Security and Applications*, vol. 76, p. 103546, Aug. 2023, doi: 10.1016/j.jisa.2023.103546.
[34] V. Khemchandani and A. Kar, "BPSK-BRO framework for avoiding side channel attacks and multiphoton attacks in quantum key distribution," *Advances in Computers. Elsevier*, pp. 41–69, 2025. doi: 10.1016/bs.adcom.2025.03.002.
[35] P. Guo, Y. Yan, F. Zhang, C. Zhu, L. Zhang, and Z. Dai, "Extending the classical side-channel analysis framework to access-driven cache attacks," *Computers & Security*, vol. 129, p. 103255, Jun. 2023, doi: 10.1016/j.cose.2023.103255.
[36] H. Wang, D. He, D. Tuo, and J. Wang, "Feature Reconstruction: Far Field EM Side-Channel Attacks in Complex Environment," in *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 10066–10081, 2025, doi: 10.1109/tifs.2025.3611788.
[37] B. Quattrone and Y. Badr, "A Survey on Acoustic Side-Channel Attacks: An Artificial Intelligence Perspective," *Journal of Cybersecurity and Privacy*, vol. 6, no. 1, p. 6, Dec. 2025, doi: 10.3390/jcp6010006.
[38] S. R. Bommana, S. Veeramachaneni, S. Ershad, and M. Srinivas, "Mitigating side channel attacks on FPGA through deep learning and dynamic partial reconfiguration," *Scientific Reports*, vol. 15, no. 1, Apr. 2025, doi: 10.1038/s41598-025-98473-3.
[39] J. Wang, X. Wang, Z. Luo, Q. Ouyang, C. Zhou, and H. Wang, "Recent Advances in Deep-Learning Side-Channel Attacks on AES Implementations," *Computers, Materials & Continua*, vol. 87, no. 1, pp. 1–10, 2026, doi: 10.32604/cmc.2025.074473.
[40] R. Benadjila, E. Prouff, R. Strullu, E. Cagli, and C. Dumas, "Deep learning for side-channel analysis and introduction to ASCAD database," *Journal of Cryptographic Engineering*, vol. 10, no. 2, pp. 163–188, Nov. 2019, doi: 10.1007/s13389-019-00220-8.
[41] G. Zaid, L. Bossuet, A. Habrard, and A. Venelli, "Methodology for Efficient CNN Architectures in Profiling Attacks," *Transactions on Cryptographic Hardware and Embedded Systems*, pp. 1–36, Nov. 2019, doi: 10.46586/tches.v2020.i1.1-36.
[42] L. Ni *et al.*, "Profiling side-channel attacks based on CNN model fusion," *Microelectronics Journal*, vol. 139, p. 105901, Sep. 2023, doi: 10.1016/j.mejo.2023.105901.
[43] C. Mujdei, L. Wouters, A. Karmakar, A. Beckers, J. M. Bermudo Mera, and I. Verbauwhede, "Side-channel Analysis of Lattice-based Post-quantum Cryptography: Exploiting Polynomial Multiplication," *ACM Transactions on Embedded Computing Systems*, vol. 23, no. 2, pp. 1–23, Mar. 2024, doi: 10.1145/3569420.
[44] K. Sheng, F. Guan, W. Ren, and T. Zhu, "T-MIA: A membership inference attack via timing side-channel and possible defense scheme," *Information Sciences*, vol. 742, p. 123317, Jun. 2026, doi: 10.1016/j.ins.2026.123317.
[45] S. Hajra, S. Saha, M. Alam, and D. Mukhopadhyay, "TransNet: Shift Invariant Transformer Network for Side Channel Analysis," *Lecture Notes in Computer Science*, pp. 371–396, 2022. doi: 10.1007/978-3-031-17433-9_16.
[46] L. Wu, G. Perin, and S. Picek, "I Choose You: Automated Hyperparameter Tuning for Deep Learning-Based Side-Channel Analysis," in *IEEE Transactions on Emerging Topics in Computing*, vol. 12, no. 2, pp. 546–557, Apr. 2024, doi: 10.1109/tetc.2022.3218372.
[47] J. Rijsdijk, L. Wu, G. Perin, and S. Picek, "Reinforcement Learning for Hyperparameter Tuning in Deep Learning-based Side-channel Analysis," *Transactions on Cryptographic Hardware and Embedded Systems*, pp. 677–707, Jul. 2021, doi: 10.46586/tches.v2021.i3.677-707.
[48] Z. Luo, M. Zheng, P. Wang, M. Jin, J. Zhang, and H. Hu, "Towards Strengthening Deep Learning-based Side Channel Attacks with Mixup," 2021 *IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 791–801, Oct. 2021. doi: 10.1109/trustcom53373.2021.00114.
[49] N. Sadeghi, M. Azghani, and S. A. Mortazavi, "Joint pilot optimization and channel estimation using deep learning in massive MIMO systems," *Digital Signal Processing*, vol. 165, p. 105287, Oct. 2025, doi: 10.1016/j.dsp.2025.105287.
[50] F. Zhang *et al.*, "Side-Channel Analysis and Countermeasure Design on ARM-Based Quantum-Resistant SIKE," in *IEEE Transactions on Computers*, vol. 69, no. 11, pp. 1681–1693, Nov. 2020, doi: 10.1109/tc.2020.3020407.
[51] S. Beck, M. Raavi, C. Dale, K. Weishalla, and B. Worrell, "Survey of Side-Channel Vulnerabilities for Short-Range Wireless Communication Technologies," *2024 IEEE International Conference on Electro Information Technology (eIT)*, pp. 450–456, May 30, 2024. doi: 10.1109/eit60633.2024.10609924.
[52] J.-W. Chang, K. Sun, D. Xia, X. Zhang, and F. Koushanfar, "EveGuard: Defeating Vibration-based Side-Channel Eavesdropping with Audio Adversarial Perturbations," 2025 *IEEE Symposium on Security and Privacy (SP)*, pp. 4534–4552, May 12, 2025. doi: 10.1109/sp61157.2025.00235.
[53] P. Wang, S. Nagaraja, A. Bourquard, H. Gao, and J. Yan, "SoK: Acoustic Side Channels," *ACM Computing Surveys*, vol. 58, no. 7, pp. 1–33, Jan. 2026, doi: 10.1145/3778350.
[54] S. Xia, L. Li, Y. Ou, and J. Xiang, "Optimizing label correlation in deep learning-based side-channel analysis," *Microelectronics Journal*, vol. 162, p. 106721, Aug. 2025, doi: 10.1016/j.mejo.2025.106721.
[55] J.-E. Woo, Y. Jeon, J.-H. Kim, and D.-G. Han, "Novel deep learning-based side-channel attack on different-device," *Soft Computing*, vol. 29, no. 8, pp. 3847–3854, Apr. 2025, doi: 10.1007/s00500-025-10610-2.
[56] Q. Li, X. Yang, and S. Ren, "A Transformer-Based Deep Learning Approach for Cache Side-Channel Attack Detection on AES," *Electronics*, vol. 15, no. 1, p. 148, Dec. 2025, doi: 10.3390/electronics15010148.
[57] X. Kou, W. Yang, L. Li, and G. Zhang, "Multi-Modal Side-Channel Analysis Based on Isometric Compression and Combined Clustering," *Symmetry*, vol. 17, no. 9, p. 1483, Sep. 2025, doi: 10.3390/sym17091483.
[58] B. Hettwer, D. Fennes, S. Leger, J. Richter-Brockmann, S. Gehrer, and T. Guneysu, "Deep Learning Multi-Channel Fusion Attack Against Side-Channel Protected Hardware," *2020 57th ACM/IEEE Design Automation Conference (DAC)*, pp. 1–6, Jul. 2020. doi: 10.1109/dac18072.2020.9218705.
[59] A. Barua, M. U. Ahmed, and S. Begum, "A Systematic Literature Review on Multimodal Machine Learning: Applications, Challenges, Gaps and Future Directions," *IEEE Access*, vol. 11, pp. 14804–14831, 2023, doi: 10.1109/access.2023.3243854.

BIOGRAPHIES OF AUTHORS

Abdul Haris Muhammad received a Bachelor of Engineering (S.T.) degree in Informatics from the National Development University Veteran Yogyakarta in 2013 and a Master of Computer Science degree from the Indonesian Islamic University, Yogyakarta, Indonesia in 2017. Currently, he is a lecturer in the Informatics Engineering Study Program, Faculty of Engineering, Universitas Muhammadiyah Maluku Utara, Ternate, Indonesia, and currently serves as the Head of the Programming Laboratory. His research interests include digital forensics, with his research specializing in malware forensics, computer vision, and cryptography. He can be contacted at email: agry.arisandi@gmail.com.

Gamaria Mandar began serving as teaching staff with the Informatics Engineering Study Program at the University of Muhammadiyah North Maluku since 2019. She is pursuing a field in natural language processing with a focus on text analysis, language modeling, and the use of AI to understand linguistic data. she is active in research, publication, and teaching activities. She can be contacted at email: gamariamandar20@gmail.com.

Adelina Ibrahim is currently an active lecturer in the Informatics Engineering Study Program, Faculty of Engineering, University of Muhammadiyah North Maluku (UMMU), Ternate, Indonesia. Obtained a Bachelor of Engineering (S.T.) in Electrical Engineering from Khairun University (UNKHAIR), Ternate (Graduated 2010), and a Master of Engineering (M.Eng.) in Information Technology from Gadjah Mada University (UGM), Yogyakarta (Graduated 2016). Deeply interested in information systems development with a special focus on software engineering and user interface design. She can be contacted at email: adelina_ibrahim@ummu.ac.id.