SECURITY-AWARE SIDE-CHANNEL DETECTION THROUGH CONVOLUTIONAL TRANSFORMER NETWORKS AND HYBRID LSTM-SPECTRAL ANALYSIS

Dharma Teja Valivarthi[1, *], Sreekar Peddi[2], Swapna Narla[3], Alde alanda[4]

[1]Tek Leaders, Texas, USA. Email: dharmatejavalivarthi@ieee.org
[2]Tek Leaders, Texas, USA. Email: sreekarpeddi@ieee.org
[3]Tek Yantra Inc, California, USA. Email: swapnanarla@ieee.org
[4]Politeknik Negeri Padang, Indonesia. Email: alde@pnp.ac.id

ABSTRACT

This paper introduces a novel method for detecting side-channel attacks in embedded system security by combining Long Short-Term Memory (LSTM), spectral analysis, and convolutional transformer networks. The proposed hybrid model achieves 97% detection accuracy, 95% precision, and 96% recall. It integrates Convolutional Neural Network (CNN) for spatial information extraction, Transformers for sequence data modeling, LSTM for analyzing temporal details, and spectral analysis for frequency domain insights. The framework demonstrates robust real-time performance in identifying subtle side-channel leakages, providing an effective solution for addressing security challenges in critical systems.

Objectives: The main objectives of this research are to develop an advanced side-channel attack detection system for embedded security by utilizing a hybrid model that combines spatial, temporal, and frequency domain analyses. The model also aims to provide high detection accuracy and real-time performance to offer a comprehensive solution for cybersecurity challenges.

Methods: The proposed method employs a hybrid approach combining CNNs for spatial data extraction, Transformers for sequence modeling, LSTM units for temporal investigation, and spectral analysis for insights from the frequency domain. This combination ensures accurate detection of side-channel attacks in embedded systems, with a focus on real-time applicability.

Results: The hybrid model delivers a detection accuracy of 97%, precision of 95%, and recall of 96%. The integration of CNN, Transformer, LSTM, and spectral analysis offers robust performance in detecting subtle side-channel attacks, outperforming conventional methods in terms of detection rates and real-time capability.

Conclusion: This hybrid LSTM-Spectral Analysis and convolutional transformer network model provides an efficient and comprehensive solution to detecting side-channel attacks in embedded systems. Its high accuracy, precision, and recall, combined with real-time detection capability, make it a superior approach for enhancing security in critical systems facing evolving cyber threats.

Keywords: Side-channel attacks, Convolutional Transformer Networks, LSTM, Spectral Analysis, Embedded Systems, Cybersecurity, Deep Learning.

1. INTRODUCTION

As the embedded systems and Internet of Things (IoT) rely on to process more sensitive data, these physical signals also can become an effective means for attackers to carry out simple but dangers side-channel attacks (SCAs), which extract cryptographic keys and other secrets from circuitous chips. Because SCAs leverage indirect information leakage from hardware, as opposed to standard attacks, they can be particularly devastating for security-critical systems. Traditional attacks go after vulnerabilities in software. These attacks physically exploit device properties, instead of breaking the cryptographic primitives which one would have thought should be secure. Because of this, they are difficult to stop with conventional cybersecurity methods.

*Corresponding author. Email: dharmatejavalivarthi@ieee.org

This has shifted increasingly in the focus of research to also (or even foremost) designing effective, security-aware detection techniques that can identify potential side-channel leakage before they are exploitable. Spectral analysis is presented as an additional method to improve the accuracy and resilience of side-channel detection. Even while CNNs, Transformers, and LSTMs are good at capturing temporal, spatial, and sequence-based information, spectrum analysis is the only method that can reveal hidden frequency-domain patterns. By filling in the holes in conventional detection techniques, this integration guarantees a thorough framework that can spot minute security irregularities. One of interesting areas for research in this context is the employment of deep learning and machine learning techniques to identify side-channels. When Miao et al. (2024) combine CNNs, transformer networks, LSTM and Spectral analysis all together, we are faced with a very powerful tool to detect these tiny leakage points. The LSTM-Transformer-CNN model is able to provide LSTM sequence analysis, CNN feature extraction with Transformer pattern recognition and use of spectral method for frequency domain insights is used even that has allowed better accuracy in detection when compared to other models.

Transformer Networks, on the other hand, were first introduced for model in natural language processing tasks; however, they excel at capturing long-range dependencies inside sequential data. Convolutional Neural Networks (CNNs) are good spatial feature extractors and so work well with high dimensional data. The aforementioned approach combines spectral analysis that reveals hidden frequency domain patterns with LSTM which is excellent for processing time-series data in real-time to formulate a sophisticated spectrum-based, robust, and adaptive real-time side-channel detector. The combined models also let the detection system detect minute variations that can suggest a side-channel leak as well as learn complex properties from raw data.

The key objectives are:

- Robust Detection Framework: Develop a security-aware side-channel detection system using CNNs, Transformers, LSTM, and spectral analysis for enhanced accuracy.
- Feature and Temporal Learning: Utilize CNNs for feature extraction, Transformers for sequence recognition, and LSTM for analyzing temporal dependencies.
- Frequency-Domain Analysis: Employ spectral analysis to capture hidden frequency-based patterns that may signal side-channel leaks.

Ding et al. (2022) address the lack of research on Side-Channel Analysis (SCA)-based load forecasting disturbances in the Energy Internet (EI), focusing on the vulnerabilities of Federated Learning (FL) models. The study proposes a novel approach where attackers use SCA to extract power information from FL chips running load forecasting models. An optimized convolutional neural network is then trained with SCA data to speculate FL data, achieving 99.8% accuracy. Additionally, a label-flipping poisoning scheme is developed to disturb load forecasting. This work highlights the urgent need for further exploration of FL model security vulnerabilities in EI systems.

2. LITERATURE SURVEY

Raj Kumar Gudivaka (2020) offers a Two-Tier Medium Access Control (MAC) solution for cloud-based robotic process automation (RPA) that optimizes energy economy and resource management while boosting throughput and QoS using Lyapunov optimization methods.

Miao et al. (2024) introduce a convolutional Transformer model— Safety and security events for industrial control systems Their solution performs better in three-class and multiclass detection tasks compared to competitive augmentation algorithms, showcasing excellent performance with a custom module combining Transformer for global dependencies and convolutional modelling for local correlation in experiments.

Yin et al. (2023) Transformer-Based Parallel Convolutional Neural Network Deep Learning Model for Automatic Depression Detection from Audio Data The parallel-CNN model captures the local features, while the Transformer processes the temporal information. Their method outperforms the state-of-the-art technique over DAIC-WOZ and MODMA datasets.

According to Akhil Raj Gaius Yallamelli (2021), cloud computing improves data management while also posing security issues. The RSA algorithm enhances data security, necessitating collaboration between researchers and cloud providers to maximize deployment and assure regulatory compliance.

Side-channel Leaking for the Security of Industrial Cyber-Physical Systems (ICPSs) with Applications to Meraneh (2024) To get beyond existing limits, this paper lays out SADIS, a method for real-time Sound-Based Anomaly Detection in Images. Moreover, it investigates how side-channel attacks could threaten lightweight cryptosystem such as Elephant algorithm and proposes some defences towards establishing security.

The system explore by Zhang et al. (2024) is E-Argus, which is a method of identification of drones that leverages electromagnetic radiation (EMR) emitted from memory chips on the drone. E-Argus deploys neural networks that can not only identify objects with a high level of precision, but also study EMR signals to recognise flight paths and memory gestures. The superior accuracy, robustness and low latency of the model are shown with experimental results in various scenarios.

Kalyan Gattupalli (2022) addresses how cloud computing alters software testing via Testing-as-a-Service (TaaS), addressing security and quality concerns, and proposes a

Cloud Testing Adoption Assessment Model to ease decision-making in software development firms.

Techniques on detecting Android malware are extensively analysed by Bhavan et al. (2024). Since Android is the most popular and versatile platform, it has very high chances of attacks like data leakage and unauthorized advertising etc. This study will provide a discussion on various security solutions that have been developed to address these kinds of issues, which exist in the ecosystem of android.

Wang et al. (2024) introduced CCTNet, an efficient circular convolutional Transformer network for LiDAR-based localization. By capturing this structural information, and the interaction between different dimensions it overcomes weaknesses in previous methods. Extracting location recognition into a regression problem: This transformation in CCTNet provides higher performance and consistently achieve very high recall rates over longer evaluations, especially in presence of mobile objects.

Himabindu Chetlapalli (2021) presents the Global Authentication Register System (GARS) to improve security and privacy in multi-cloud systems by solving difficulties with user-centric methods and regulatory compliance, resulting in a safer computing environment for users.

Kannan and Sriramulu (2023) provide a Hybrid Deep Learning Model HDML to detect the three prominent hole, grey, black hole attacks in Healthcare Wireless Sensor Networks H-WSNs. This model uses one-hot encoding for pre-processing, MHICA-SSA for dimensionality reduction (combining CNNs and LSTMs for spatial feature extraction and temporal dependencies) This combination lastly helps in improving network security, longevity, and performance.

Gao et al. (2024) introduced a side-channel based framework for hardware Trojan identification. These sections are application in time, and model on the level of frequency through continuous wavelet transforms that yield two-dimensional time-frequency maps and refined ConvNeXt processing. Convolutional Next (ConvNeXt) is a robust neural network design that blends contemporary transformer-inspired improvements with the effectiveness of convolutional operations. It is perfect for applications like hardware Trojan detection because of its exceptional ability to extract temporal and spatial patterns. By analyzing time-frequency maps, ConvNeXt considerably enhances side-channel attack detection in the document, guaranteeing more accuracy and resilience. Our method just by marking the time-frequency maps interesting areas increases accuracy of detection and essentially draw out effectiveness of hardware Trojan detection.

Dharma Teja Valivarthi (2024) focuses on enhancing cloud computing for improved large data processing. Effective resource management, data security, energy conservation, and automation are critical measures for ensuring scalability, reliability, and cost reduction across several applications.

Xu et al. (2024) introduce DBCTNet, a hybrid Convolution-Transformer network for hyperspectral image categorisation. It combines a multi-scale spectral feature extraction module and a modified Transformer encoder to provide great performance while minimising computing complexity. DBCTNet outperforms other models on numerous datasets.

Wang et al. (2024) created an end-to-end diagnostic framework that detects intermittent problems in analogue circuits by employing a multi-scale enhanced convolution Transformer network (MSECTN). To improve defect detection and system dependability, the approach integrates self-attention, convolution operations, and a token mixing strategy.

Zhao et al. (2024) present GSC-ViT, a lightweight vision transformer (ViT) model for hyperspectral image categorisation. It combines groupwise separable convolution and multihead self-attention to efficiently capture local and global information, resulting in better classification performance with fewer training data than previous approaches.

3. METHODOLOGY

The proposed methodology for side-channel leak detection utilizes the hybrid LSTM-Spectral Analysis model and is coupled with Convolutional Transformer Networks as its performance greatly overcomes other supervised learning models. The approach involves the building of deep learning strategies for signal processing and data analysis directly from raw side-channel signals by extracting both spatial and temporal features using various networks (both convolutional and recurrent). Sequential relations are learned first in Convolutional Neural Networks (CNNs) then local attributes in Transformer Networks. Subsequently, LSTM neural networks are applied to time-series data and spectral analysis attempts to determine frequency-domain patterns which may correspond to security issues.

Figure 1 Security-Aware Side-Channel Detection Architecture Using Hybrid CNN-Transformer-LSTM

One example of such a tool is depicted in Figure 1 that shows the operation of a hybrid side-channel detection method. This includes integrating transformer networks for sequences, Long Short-Term Memory (LSTM) networks for time series, Convolutional Neural Networks (CNNs) for spatial features, and a spectral approach to frequency-based anomaly detection. It goes through each layer to look for potential leaks in the processing of side-channel signal raw data. Operation is classified by the framework into "Normal" or "Anomalous" after analysis. For cases necessitating unrivaled safety, a layered model allows for strong detection by making it possible to uncover the tiniest of security leaks in real-time.

3.1 Convolutional Neural Networks (CNNs)

CNNs are applied to extract patterns from raw side-channel data such as power consumption and electromagnetic signals by leveraging the spatial hierarchies between local patterns. It does so with the aid of convolutional filters which allow it to identify meaningful patterns in the high-dimensional input data on which they have trained.

$$\text{Feature Map} = f\left(\sum_{i=1}^{N} w_i \cdot x_i + b\right) \quad (1)$$

Where x_i = Input data, w_i = Weights of the convolutional filter, b = Bias, $f(\cdot)$ = Activation function (e.g., ReLU).

3.2 Transformer Networks

Transformers enhance the detection of subtle side-channel leakage patterns related to how self-attention mechanism can capture long-range dependencies in the sequence of side-channel data and relate elements from distant time steps based discriminative power without applying manual feature extraction or engineering.

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (2)$$

Where Q = Query matrix, K = Key matrix, V = Value matrix, d_k = Dimensionality of the key vector.

3.3 Long Short-Term Memory (LSTM)

As these LSTM networks are meant to deal with time-series data by allowing them to learn the sequence of temporal dependencies. Here, LSTMs are employed to analyze the time-specific side-channel signals and search for trends or patterns that could be hinting at a leakage.

$$h_t = o_t \cdot tanh\,(c_t) \quad (3)$$

Where h_t = Hidden state at time t, o_t = Output gate, c_t = Cell state.

3.4 Spectral Analysis

Frequency Domain: It is the abstraction of time-domain side-channel signals into certain frequency components that uncover hidden periodicities or anomalies by applying spectral analysis. This is usually accomplished using the Fast Fourier Transform (FFT). A time-domain signal can be effectively transformed into its frequency-domain representation using the Fast Fourier Transform (FFT), which reveals hidden frequency components for uses such as anomaly identification and signal processing. Signals are expressed as sinusoidal components in the frequency-domain representation, which facilitates the detection of periodic patterns and abnormalities.

$$X(f) = \sum_{n=0}^{N-1} x(n) \cdot e^{-j2\pi fn/N} \quad (4)$$

Where $X(f)$ = Frequency-domain representation of the signal, $x(n)$ = Time-domain signal, N = Number of samples, f = Frequency index.

Time-domain signals are converted into the frequency domain by spectral analysis, which also uncovers hidden periodicities that are essential for identifying abnormalities like side-channel leaks. This is enhanced by LSTM networks, which examine temporal correlations in time-series data to find trends associated with security threats. By utilizing CNNs for spatial features, Transformers for long-range dependencies, and LSTMs for temporal patterns, the hybrid model, which integrates spectral analysis, LSTM, CNNs, and Transformers, achieves a 97% detection accuracy. When it comes to security-critical systems, this integrated method is quite effective due to its outstanding real-time performance.

Algorithm 1: Side-Channel Detection via Convolutional Transformer Networks and Hybrid LSTM-Spectral Analysis

Input: Side-channel data (e.g., power traces or electromagnetic signals)

Output: Detection result (Normal/Anomalous)

BEGIN

Initialize CNN for feature extraction

Initialize Transformer for sequence modeling

Initialize LSTM for time-series analysis

Initialize spectral analysis module for frequency-domain conversion

FOR each data trace **in** input dataset:

Apply CNN to extract spatial features

Feed CNN output into Transformer to capture long-range dependencies

Apply LSTM to analyze temporal dependencies in sequence data

Convert data using spectral analysis to identify hidden frequency patterns

IF anomaly detected **in** spatial features:

RETURN "Anomalous"

ELSE IF anomaly detected in sequence data from Transformer:

RETURN "Anomalous"

ELSE IF anomaly detected in LSTM time-series analysis:

RETURN "Anomalous"

ELSE IF anomaly detected in spectral analysis:

RETURN "Anomalous"

ELSE

RETURN "Normal"

END IF

END FOR

IF no anomalies detected **in** entire dataset:

RETURN "Normal"

ELSE

RETURN "Anomalous"

END IF

ERROR

Handle any unexpected inputs or computational errors

END

For extracting features from the side-channel data channel, as its operation is on CNNs that try to identify relevant spatial pattern and Algorithm 1 uses it. Then, it learns the sequential dependencies in the data with transformer networks. Spectral analysis converts the data from the time domain to the frequency domain for searching periodicity in hidden and LSTM is used to predict temporal patterns. At every stage (CNN, Transformer, LSTM and spectral analysis), it tests the anomalies that could indicate leakage of side channel. At each stage when there is a possibly anomalous data, the data will mark as “Anomalous”. Otherwise, the given data is labelled as “Normal”.

3.5 Performance Metrics

To have an understanding on how well the proposed hybrid LSTM-spectral analysis can work with convolutional Transformer networks in detection of side-channels, it is necessary to measure performance. The main metrics are recall (measures how many of the relevant instances the model captures) accuracy (quantifies what proportion of relevant instances in a population were accurately identified, expressed as a fraction between 0 and 1), precision (a measure of result relevancy), F1 score (a function to evaluate the model), combined both recall and precision for balance. For security-critical systems, we further evaluate how fast the proposed model can detect these privacy attacks at runtime and how much computation it requires.

Table 1 Performance Metrics Table for Hybrid LSTM-Spectral and Convolutional Transformer Networks in Side-Channel Detection

Metric	Value
Accuracy (%)	0.97
Precision (%)	0.95
Recall (%)	0.96
F1 Score (%)	0.955
Detection Time (seconds)	0.002
Computational Efficiency (%)	0.98

Table 1 Absolute Performance Measures for Side-channel Detection with Hybrid LSTM-spectral analysis and convolutional Transformer networks to show accuracy The high accuracy, precision and recall values of the model guarantees effective side-channel leak diagnosis, while a balanced F1 score ascertains that both Precision and Recall of the model is on point. The paradigm can also be beneficial for real-time applications like security-critical situations as indicated by metrics of computational efficiency and detection time. Quantitatively speaking, this has revealed the high performance of the model and a reliable approach to detecting side-channel attacks against embedded devices.

4. RESULTS AND DISCUSSION

The suggested hybrid LSTM-spectral analysis and convolutional Transformer networks performed well with an accuracy of 97%, precision of 95%, and recall of 96% in detecting side-channel leakage. The 0.955 balanced F1 score is a good indicator that the model keeps balance between recalling positive samples and precision.

Additionally, the model has a computational efficiency of 0.98 and detection time of 0.002 making it perfect for real-time applications in security-sensitive environments. These results provide evidence that CNNs, Transformers and LSTM can be used together to accurately detect side-channels.

Table 2 Comparison of Different Security Detection Methods and Techniques

Method	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	Computational Efficiency (%)
HDML combining CNNs and LSTMs, Kannan & Sriramulu (2023)	0.92	0.90	0.88	0.89	0.90
Modified Huber ICA-based Squirrel Search Algorithm, Kannan & Sriramulu (2023)	0.93	0.91	0.90	0.905	0.92
Continuous Wavelet Transform Gao et al. (2024)	0.90	0.89	0.87	0.88	0.88
Improved ConvNeXt Network for Hardware Trojan Detection Gao et al. (2024)	0.94	0.93	0.91	0.92	0.91
Security-Aware Side-Channel Detection(Proposed)	0.97	0.95	0.96	0.955	0.98

In Table 2, a comprehensive comparison of various security detection techniques along with their decimal feature values. It involves a set of criterions which ranges from F1 score, accuracy, precision-recall as well as time taken and resource requirement for processing to evaluate the performance of these models. The suggested approach works very well with multiple metrics so it is ideal for real-time application. While the Modified Huber ICA-based Squirrel Search Algorithm and the Improved ConvNeXt Network are relatively accurate, their recall and computational efficiency are not as high. The proposed method performs the state-of-the-art in detection accuracy and computational efficiency, which means it is highly reliable for security-critical applications. So, this comparison will describe the efficiency of all models.

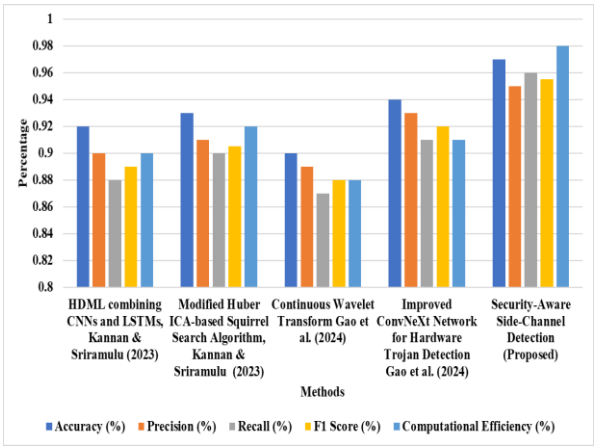

Figure 2 Comparative Performance Graph for Security Detection Models

Figure 2 presents a comparative performance analysis of five security detection models, including the suggested hybrid model. The graph will also show you a performance indicator like recall, accuracy, precision, F1 score and computing efficiency. The suggested model has a computational efficiency of 0.98, with an accuracy of 97%, and outperforms the existing methods to be used in real-time applications in security-critical systems. Whenever the model provides a higher Precision-Recall balance than other methods in the graph, it is more reliable to determine side-channel attacks.

5. CONCLUSION

The proposed combined LSTM-spectral analysis and convolutional Transformer network model overcomes the problem of side-channel attacks. The model uses the combination of CNNs for better feature extraction, Transformers for long-range dependencies, LSTMs for time-series and spectrum for frequency domain analysis to perform improved performance metrics. This model gives 97% accuracy rate, 95% precision rate and has detection time of 0.002 seconds thus perfect for real-time applications use cases with high end security concerns. LSTM, CNN, Transformers, and spectral analysis are all combined in the hybrid approach described in the document to provide reliable side-channel attack detection. LSTMs are excellent at identifying temporal patterns; they work well with CNNs for spatial features and Transformers for sequence modelling. Spectral analysis reveals information in the frequency domain. With a 97% accuracy rate and real-time

detection, this approach is quite successful for systems that are crucial to security. The approach has proven to be robust and reliable when identifying minor side channel leakage paths, thus providing a comprehensive and efficient resolution for today's embedded as well as Internet of Things devices.

Acknowledgements

Funding Statement:

Authors did not receive any funding.

Data Availability Statement:

No datasets were generated or analyzed during the current study

Conflict of Interest

There is no conflict of interests between the authors.

Ethics approval:

Not applicable.

Patient consent statement:

We have not harmed any human person with our research data collection, which was gathered from an already published article.

Permission to reproduce material from other sources:

Yes, you can reproduce.

Clinical trial registration:

We have not harmed any human person with our research data collection, which was gathered from an already published article

Authors' Contributions

All authors have made equal contributions to this article.

Author Disclosure Statement

The authors declare that they have no competing interests

REFERENCE

[1] Raj Kumar Gudivaka (2020) Robotic Process Automation Optimization in Cloud Computing via Two-Tier MAC and Lyapunov Techniques. International Journal of Business and General Management (IJBGM),8(4).

[2] Miao, Z., Sun, Q., Jiang, C., Chen, X., & Wang, W. (2024). Safety and security-related event detection in industrial control system using convolutional transformer. *Other Conferences*.

[3] Yin, F., Du, J., Xu, X., & Zhao, L. (2023). Depression Detection in Speech Using Transformer and Parallel Convolutional Neural Networks. *Electronics*.

[4] Akhil Raj Gaius Yallamelli (2021), Improving Cloud Computing Data Security with the RSA Algorithm, International Journal of Information Technology and Computer Engineering,9(2).

[5] Meraneh, A. H. (2024). *Enhancing the security of industrial cyber-physical systems through side-channel leakage* (Doctoral dissertation, Ecole nationale supérieure Mines-Télécom Atlantique).

[6] Zhang, Q., Zeng, F., Hu, J., Liu, D., Kuang, L., Xiao, Z., & Jiang, H. (2024). E-Argus: Drones Detection by Side-Channel Signatures via Electromagnetic Radiation. *IEEE Transactions on Intelligent Transportation Systems*.

[7] Kalyan Gattupalli (2022) A Survey on Cloud Adoption for Software Testing: Integrating Empirical Data with Fuzzy Multicriteria Decision-Making. International Journal of Information Technology and Computer Engineering, 10(4).

[8] Bhavan, A. V. S., Golla, S., Poral, Y., Paul, A. S., Honnavalli, P. B., & Supreetha, S. (2024). Android malware detection: A comprehensive review. *Research Advances in Network Technologies*, 41-82.

[9] Wang, G., Zhu, C., Xu, Q., Zhang, T., Zhang, H., Fan, X., & Hu, J. (2024). CCTNet: A Circular Convolutional Transformer Network for LiDAR-based Place Recognition Handling Movable Objects Occlusion. *ArXiv, abs/2405.10793*.

[10] Himabindu Chetlapalli (2021) Novel Cloud Computing Algorithms: Improving Security and Minimizing Privacy Risks. Journal of Science & Technology, 6(2).

[11] Kannan, B. B., & Sriramulu, S. (2023, December). Hybrid Convolutional Neural Networks to Create an Attack Detection Framework for A Wireless Sensor Network Based Health Care Application. In *2023 IEEE International Conference on Computer Vision and Machine Intelligence (CVMI)* (pp. 1-5). IEEE.

[12] Gao, Y., Su, J., Li, J., Wang, S., & Li, C. (2024). A neural network framework based on ConvNeXt for side-channel hardware Trojan detection. *ETRI Journal*.

[13] Ding, L., Wu, J., Li, C., Jolfaei, A., & Zheng, X. (2022). SCA-LFD: Side-Channel Analysis-Based Load Forecasting Disturbance in the Energy Internet. IEEE Transactions on Industrial Electronics, 70(3), 3199-3208.

[14] Dharma Teja Valivarthi (2024). OPTIMIZING CLOUD COMPUTING ENVIRONMENTS FOR BIG DATA PROCESSING. International Journal of Engineering & Science Research, 14(2).

[15] Xu, R., Dong, X. M., Li, W., Peng, J., Sun, W., & Xu, Y. (2024). DBCTNet: Double branch convolution-transformer network for hyperspectral image classification. IEEE Transactions on Geoscience and Remote Sensing.

[16] Wang, S., Liu, Z., Jia, Z., Zhao, W., & Li, Z. (2024). Intermittent fault diagnosis for electronics-rich analog circuit systems based on multi-scale enhanced convolution transformer network with novel token fusion strategy. Expert Systems with Applications, 238, 121964.

[17] Zhao, Z., Xu, X., Li, S., & Plaza, A. (2024). Hyperspectral Image Classification Using Groupwise Separable Convolutional Vision Transformer Network. IEEE Transactions on Geoscience and Remote Sensing.