University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

Enhancing Cryptographic Security Through a Machine Learning Model for Early Detection of Side-Channel Attacks

Zainab Rustum Mohsin

College of computer science and Mathematics, University of Thi-Qar ,Thi-Qar 64001,Iraq

Email :zainabrustum@utq.edu.iq

Abstract

This paper presents a profiling method of side-channel leakage of AES algorithm desynchronized traces based on the ASCAD dataset using deep learning devices. The model relies on a convolutional neural network (CNN) design to automatically derive useful features of the time-series measurements of power, surmounting the noise and keep-up issues.

As shown by experiment, the proposed model has a high training accuracy of 95.4% and a validation accuracy of 95.1% when the number of epochs reached 60, which means that the model has achieved good generalization and adaptability to irregular and noisy data. The model manages to find pattern relations that are related to the secret key bytes, which shouldn't be underestimated as to the possibility of deep learning to improve side-channel analysis even in very difficult circumstances.

These results imply the relevance of machine learning to cryptographic security and inform about the efficiency of attacks.

Key words: Side-Channel Analysis (SCA), Deep Learning, Convolutional Neural Networks (CNN), Power Analysis, ASCAD Dataset

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

1. Introduction

Modern encryption techniques, such as AES and the RSA algorithm, are characterized by their mathematical robustness and are among the most reliable and effective methods for securing and protecting sensitive information within digital systems [1]. In real-world applications, particularly in embedded systems, microcontrollers, and Internet of Things (IoT) architectures, cryptographic algorithms can be compromised by vulnerabilities arising from the physical environment in which they operate. This has led to the emergence of what are known as side-channel attacks, a class of attacks in which attackers exploit unintended leaks from the physical world, such as power consumption patterns, execution time variances, or electromagnetic emissions during cryptographic operations [2].

Side-channel attacks represent a fundamental shift in the security threat landscape. In these attacks, the attacker focuses not on the mathematical foundations of the encryption algorithm, but rather on analyzing the internal behavior of the device executing it. This approach allows for the extraction of sensitive information, particularly encryption keys, with unexpected efficiency, even when the algorithm itself is theoretically secure. As the effectiveness of these attacks has been demonstrated against commercial smart cards, embedded processors, and various consumer devices, their severity and prevalence are steadily increasing [3].

To address these analyzed challenges, researchers and hardware designers rely on well-known countermeasures such as masking, hiding, noise, and random delays. While effective in some scenarios, these techniques can place an additional burden on performance, increase hardware design complexity, and, in some cases, are incompatible with advanced analysis techniques. Furthermore, most available countermeasures do not detect the attack itself but merely attempt to reduce the amount of leaked information,

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

rendering systems unable to recognize or respond to ongoing attacks in a timely manner until the attacker ultimately manages to extract the secret key [4].

The new development of machine learning (particularly deep learning) is capable of providing another paradigm of reasoning side-channel information. Specifically, CNNs are highly beneficial in the pattern recognition and analysis of signals, significantly enticing the subtle variations in signal traces in power that can be missed by classical statistical techniques. Such capabilities allow early warning mechanisms, which trace the power over time and detect abnormal behavior suggesting a side-channel attack with an ideal outcome of detecting it before much leakage is spent.

This study examines this new direction by constructing and testing a machine learning model that can detect an attack on side-channel by analyzing power traces data. Standardized datasets like ASCAD dataset give a controlled and repeatable environment to train and evaluate such models and are thus suitable benchmarks to academic research and experimental validation.

This work is inspired by a number of observations:

- Side-channel attacks are feasible, cost-effective and very effective.
- Sensors Small embedded devices frequently employed in security critical applications do not have high level monitoring.
- On the side-channel analysis, machine learning models have also performed better, and this implies that the same can be used to detect as opposed to attack.
- Key recovery can even be avoided ahead of time providing a greater line of defense as compared to the traditional means:

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

Although earlier researchers have put their efforts in applying deep learning to carry out side-channel attacks (i.e. to recover keys), a much smaller number of researchers applied the concept of applying machine learning to side-channel attack detection.

In particular, there is a lack of the existing literature:

- ML-based models that can be used in real-time or early detection.
- Evaluations that measure detection performance under noise and desynchronization
- Frameworks that present side-channel detection as classification problem.
- Standardization Tests Experiments directed at standardized datasets like ASCAD.
- This research fills this gap.

This research aims to:

- Analyze power-consumption traces extracted from cryptographic operations and identify distinguishable patterns
- Develop a machine-learning model—based on deep learning architectures—to Early Detection of Side-Channel Attacks
- Measure the performance of the models in standard measures like accuracy.
- Offer an opinion as to whether machine learning can be a pertinent instrument in at an early stage identically detecting attack vulnerabilities on an embedded cryptographic framework.

2. Problem Statement

Even though the cryptographic algorithms are highly mathematically secure, their physical implementations provide information that can be use-oriented by the attacker. The current security measures lack early warning and smart observation. In this way,

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

systems are susceptible to SCAs that can be code-snort and steal the secret key before the defense mechanism can do so.

The most important issue that was tackled in the research is that, there was lack of a machine-learning-based system that would be able to examine power traces and determine the presence of a side-channel attack in progress on an early stage.

3. Theoretical Background

3.1 Side-Channel Leakage Fundamentals

White-box side-channel analysis (SCA) relies on exploiting physical leaks from cryptographic devices during algorithm execution. These leaks include power consumption, electromagnetic emissions, and execution time variances, which collectively reflect internal data processing within the hardware. Since digital circuit switching depends on the values being processed, certain measurement patterns can be linked to sensitive intermediate states during cryptographic operations [5].

3.2 Leakage Modeling in Cryptographic Devices

Several analytical models are used to explain physical leaks, most notably the Hamming Weight (HW) and Hamming Distance (HD) models. The HW model relates power consumption to the number of bits set to 1, while the HD model focuses on the number of transitions between two consecutive bit states during processing. These models provide a conceptual framework that links the physical behavior of hardware to the mathematical operations performed by cryptographic algorithms such as AES [6].

3.3 Profiling Attacks and the Supervised Learning Setting

In profiling attacks, the attacker is assumed to possess a device identical to the target device. A large number of measurement traces are collected using known keys, and the attacker then creates a supervised classifier trained to associate physical leaks with

sensitive intermediate values. Standardized datasets, such as ASCAD, are specifically used to test this type of attack, making them a cornerstone of modern side-channel analysis research [7].

3.4 Challenges Introduced by Desynchronization Countermeasures

Several real-world realizations have anti-measures to hide leakage characteristics. The particularly disruptive one is the desynchronization, as such presents random shifts or jitter among the traces. This discrepancy renders the process of identifying the same leakage point using traditional attack forms especially difficult in different traces greatly impairing their effectiveness.

3.5 Limitations of Classical Statistical Attacks

Conventional methods such as Correlation Power Analysis (CPA) or template attacks rely on precise alignment and predefined points of interest. When traces are misaligned or noisy, these approaches struggle to extract consistent features. Their reliance on handcrafted preprocessing makes them less adaptable to countermeasures like desynchronization.

4. Literature Review

This paper examines vulnerabilities in the side-channel attacks on the AES algorithm based on cache vulnerabilities. The hardware performance counters applied by the authors to mine the features related to various events of the cache are under (Flush and Reload), (Prime and Probe), and (Flush and Flush) attack scenarios. First, a random forest algorithm is used to identify the most relevant cache features which help to eliminate noise and enhance features quality. Then, a support vector machine (SVM) model is trained to identify attack and non-attack traces. The research shows extremely high levels of detection: 99.92 in the idle system, 99.85 in moderate system load condition and 96.57 in the full loading system condition. One of the key concepts in this work is the role of

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

combining effective feature selection with supervised learning models in achieving an accurate detection of side-channel in especially hardware-level attacks [8].

In this paper, the authors discuss the application of deep learning and specifically convolutional neural networks (CNNs) to pursue profiling attacks on AES implementations. They highlight the relationship between deep learning methods and conventional template attacks and demonstrate that hierarchical features of electromagnetic (EM) traces are automatically retrieved by CNNs. They, in a first analysis, methodically treat the choice of the best network parameters to be used with convolutional models in the analysis of side channels, on a data set, named ASCAD, that gives both fixed-key and random-key traces. The ASCAD dataset is a reproducible one because all target implementations and measured EM traces are contained in it. It is seen that deep learning models, such as VGG-inspired CNN models, attain high profiling accuracy without any activity-controlled feature-extraction as is the case with traditional attacks [9].

This article presents a deep learning architecture, known as 2Deep, aimed at parallel code executions of post-quantum key exchange protocols (Frodo and NewHope). The most important innovation is the fact that the 1-D time-series power traces can be converted into 2-D images and thus transforming the entire side-channel analysis into an issue of image recognition. Through this method, the authors show that they have made a significant enhancement to the preexisting methods, which are: horizontal differential power analysis (DPA), template attacks and naive 1-D deep learning models. The 2-D approach to profiling is capable of improving the probability of attack success, but also cross-device profiling, enabling the use of a model trained on one device to provide extrapolation to other devices. As an example, the attack against Frodo became more successful, 20% (1-D) to 99% (2-D), which corresponds to the prospects of the spatially-encoded representations and data augmentation in the contemporary side-channel attacks [10].

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

The paper is a first use of deep learning to profile attacks on the small cryptography algorithm SPECK-32/64. The authors use a round-based, byte-level divide-and-conquer algorithm, which maximizes the key recovery process by paying attention to intermediate subkeys at each round. They use a fixed-key and variable-key dataset in their experiments to confirm the approach. Exceedingly, the approach has attained complete key recovery with less than 250 traces and effective correct judgments are realized after the initial four rounds of the cipher. The paper proves the effectiveness of deep learning-based implementation of lightweight cryptographic primitives and highlights that even a small amount of traces can be used effectively to attack them successfully with an appropriate use of hierarchical neural network models[11].

This study suggests a systematic approach to detect side-channel attacks with the classical machine learning technique. The process starts with the data collection and involves the preprocessing procedures involving the reduction of noises, normalization as well as the segmentation. Both statistical and frequency-domain analysis in the form of Quick Fourier Transform (FFT) coefficients are used to extract the relevant features. Then, a SVM model is trained to differentiate attack and non-attack traces. It demonstrates that the accuracy of classifying the classification is 88 percent on the validation set, where frequency-domain features were found to be the most significant ones. This paper highlights the significance of preprocessing and feature engineering in machine learning-based side-channel detection and has a distinct comparison with the new deep learning solutions [12].

the suggested methodology in [14], InfoNEAT is based on the principle of neural structure search, with the aid of information-theoretic measures that help to optimize the evolution, early terminate it with new stopping criterion, and reduce time-complexity and memory footprints. The effectiveness of the InfoNEAT is determined through utilizing it on publicly accessible datasets of real measurements in side channels. Besides the significant benefits on the basis of the automated configuration of NNs, InfoNEAT shows

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

significant performance improvements over the other methods of optimal key recovery in terms of the number of epochs (e.g.,x6 faster), the number of attack traces to break a device (up to 1000s fewer), and the reduction in the number of trainable parameters over MLPs (by the factor of up to 32). In addition, it is proven with experiments that InfoNEAT models can survive noises and trace desynchronization.

In [15], the authors suggested, a physical design level PSC evaluation model very fast and efficient with the help of a graph neural network (GNN). This framework predicts the traces of dynamic power of new layouts and it uses them to evaluate security of physical design using metrics. Experiments of AES-GF layout implementation of our work with impressive 133 speedup over traditional simulation-based flow and no significant loss of accuracy.

Another novel method to know side-channel attacks that integrate active learning based machine learning models, namely, Random Forest, eXtreme Gradient Boosting, Decision Tree, Gradient Boosting, K-Nearest Neighbors and Light Gradient-Boosting Machine classifier are proposed in paper [16]. The method is tested on a dataset created using hardware sensors of the smartphone (i.e. accelerator, gyroscope and magnetometer). The performance is tested in three rounds; the evaluation measures indicate that the assignment of the keystrokes can be assessed with the following accuracy of 91.99 and with the F1-score of 91.89. The results suggest that the method is extremely precise and elucidates the rate of inferences efficiently to gauge attacks as opposed to traditional non-ML techniques and other existing studies.

A comparison of past studies and present studies is drawn in table 1.

Table 1 comparison table

Study	Method	Key Findings	Relevance to Our Work
[8]	Random Forest + SVM	Detection accuracy 96–99.92% under different system loads	Demonstrates effective feature selection and classical ML for SCA, emphasizes preprocessing importance

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

[9]	CNN / DL	Open database, CNN profiling, high accuracy	Provides standardized dataset and CNN framework for AES profiling, aligned with our approach
[10]	1D→2D DL	Data transformation boosts attack success, cross-device attacks	Illustrates benefit of trace transformation and data augmentation, inspires improvements in input representations
[11]	DL profiling	Full key recovery with <250 traces, first 4 rounds sufficient	Validates byte-level, round-based profiling with DL, demonstrates efficiency in lightweight ciphers
[12]	SVM	88% classification, FFT features key	Highlights importance of preprocessing, statistical and frequency-domain feature extraction
[14]	neural structure	demonstrated that InfoNEAT's models are robust against noise and desynchronization in traces	InfoNEAT shows significant performance improvements over the other methods of optimal key recovery in terms of the number of epochs (e.g.,x6 faster)
[15]	graph neural network (GNN)	133× speedup compared to conventional simulation-based flow	Demonstrates effective of DNN
[16]	Random Forest, eXtreme Gradient Boosting, Decision Tree, Gradient Boosting, K-Nearest Neighbors, and Light Gradient-Boosting	accuracy of 91.99% and F1-score of 91.89%	Demonstrates effective of classical ML for SCA
Our Work	CNN + PCA	Dimensionality reduction via PCA, one-hot encoding labels, tailored CNN	Extends prior DL SCA studies with PCA for feature compression and CNN optimization for profiling accuracy on fixed-key AES

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

5. Methodology

Each measured power trace xi can be expressed as the sum of a data-dependent leakage component and noise:

xi = L(zi) + ni

where xi represents the measured power trace, L(.) is the leakage function, and ni denotes measurement noise.

The sensitive intermediate variable zi is defined as:

zi = SBox(pi XOR k)

where pi is the plaintext byte and k is the secret key byte.

A convolutional neural network is trained to learn a function f that maps a power trace to the corresponding sensitive value:

zi_hat = f(xi)

The network outputs a probability distribution over all possible classes, and the secret key is determined by selecting the key hypothesis that maximizes the accumulated likelihood over multiple traces.

5.1 Dataset Description [13]

- The experiment utilizes the ASCAD Fixed-Key dataset, which is power traces of AES cryptography of bits transmitted on an embedded microcontroller.
- The dataset will have several degrees of desynchronization (e.g., 0, 50, 100) in order to have some realistic conditions in which the traces can be not perfectly aligned.
- The data will be split into training and testing.
    - Training traces: 50,000 samples

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

- Testing traces: 10,000 samples

- Every trace illustrates the power consumption of the device with time taken during the encryption of AES.

5.2 Data Preprocessing

A carefully devised preprocessing pipeline on the ASCAD fixed-key traces was performed before model training to maintain the data consistency, dimensionality reduction, and ready the leakage samples to be analyzed using deep learning, allowing the use of the side-channel analysis. The data includes profiling and attack traces in an HDF5 format, and other metadata, including plaintext, key bytes, and masking values. The preprocessing method adopted in this work is a summary of the steps listed below as depicted in figure 1:

5.2.1. Dataset Loading and Structure Extraction

The attack subsets and profile were loaded directly out of the HDF5 file such as:

- Raw power traces
- Label values representing the S-box output of the targeted intermediate state
- Plaintext and key metadata
  This ensures that all information required for supervised leakage modeling is correctly aligned and accessible.

5.2.2. Consistency Inspection

Simple integrity assurance was done through inspecting array shapes, printing sample traces. This is done in order to ensure that the loaded labels actually reflect the desired class of leakage.

5.2.3. Signal-to-Noise Ratio (SNR) Exploration

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

A SNR curve was calculated prior to training to find the time samples that have significant data-dependent leakage.

Even though no manual feature selection was used, SNR visualization can give one insight into which parts of the traces have potentially useful information to key recovery and verify that the dataset format is also somewhat as expected leakage traces.

5.2.4. Dimensionality Reduction via PCA

Because the traces chosen originally have 700 time samples per trace, Principal Component Analysis (PCA) was utilized to reduce the traces and retain most of the variance.

The PCA filters out duplicate or noise-heavy elements using a 0.995 retained-variance and provides a representation of the data size that is smaller in magnitude and thus speeds up the training process and makes the model more stable.

5.2.5. Input Reshaping for the Neural Network

The samples after PCA transformations were reshaped into convolutional architecture format.. Each trace is represented as a 1-dimensional sequence of principal components with a single feature channel, enabling effective feature extraction through 1D convolution.

5.2.6. Label Encoding

Categorical encoding was used to transform the labels of the scalar class to one-hot vectors.

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

5.2.7. Train–Validation Splitting

In order to check the performance of a model and prevent overfitting, 20 percent of the profiling data was kept in a validation set at the time of training. This gives a fair estimate of the generalization functioning in the company prior to the final attack phase.

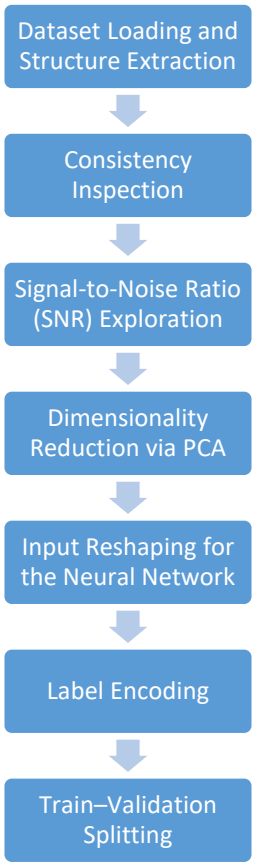

Figure 1 Data Preprocessing

5.3 Model Architecture

- An automatic learning of the discriminative features of the traces in the form of a Convolutional Neural Network (CNN) is employed.
- Typical architecture includes:

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

- Multiple 1D convolutional layers to extract local patterns from the power traces.
- Activation functions such as ReLU.
- Pooling layers to reduce dimensionality.
- Fully connected layers to map features to the trace labels.
- Softmax layer for classification.

- The model is trained using a **categorical cross-entropy loss function** and optimized using the **Adam optimizer**.

5.4 Training Procedure

- **Train/Test Split:** Training set (50,000 traces) and test set (10,000 traces).
- **Batch size:** Optimized to balance memory usage and convergence speed.
- **Number of Epochs:** Selected based on convergence of loss and validation accuracy.
- **Evaluation Metrics:**
  - Accuracy: proportion of correctly classified traces.

5.5 Implementation Tools

- Python programming language with libraries such as **NumPy**, **h5py**, **TensorFlow/Keras**, and **Matplotlib** for visualization.
- The model is trained and evaluated on Google Colab or local GPU-enabled environments.

5.6 Experimental Workflow

1. Load the ASCAD dataset.
2. Preprocess and normalize the traces.
3. Split data into training and testing sets.

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

4. Build the CNN model architecture.
5. Train the model on the training set.
6. Evaluate the model on the testing set using accuracy, loss, and confusion matrix.

Figure 2 show Experimental Workflow.

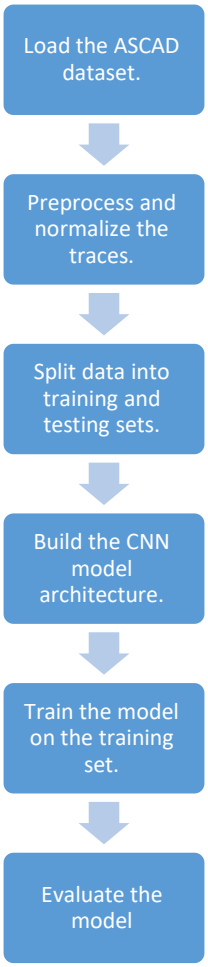

Figure 2 Experimental Workflow

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

6. Result and discussion

Figure 3 illustrates the layers of the model that were trained and tested, and shows the trainable parameters.

Layer (type)	Output Shape	Param #
conv1d (Conv1D)	(None, 539, 32)	384
batch_normalization (BatchNormalization)	(None, 539, 32)	128
max_pooling1d (MaxPooling1D)	(None, 269, 32)	0
conv1d_1 (Conv1D)	(None, 269, 64)	14,400
batch_normalization_1 (BatchNormalization)	(None, 269, 64)	256
max_pooling1d_1 (MaxPooling1D)	(None, 134, 64)	0
flatten (Flatten)	(None, 8576)	0
dense (Dense)	(None, 256)	2,195,712
dropout (Dropout)	(None, 256)	0
dense_1 (Dense)	(None, 128)	32,896
dense_2 (Dense)	(None, 256)	33,024

Total params: 2,276,800 (8.69 MB)
Trainable params: 2,276,608 (8.68 MB)
Non-trainable params: 192 (768.00 B)

Figure 3 model layers

Figure 4 shows Signal-to-noise ratio (SNR) analysis performed on the collected power paths revealed significant leakage in the AES application. The calculated SNR values ranged from approximately 1.1 to 1.7 across 700 time points. These values indicate a moderate level of information leakage, with some samples showing statistically significant variations related to the mean value. Although the leakage is not extremely severe, it is significant enough to confirm that the encryption device is unintentionally revealing key-dependent behavior, making it possible for machine learning-based side-channel analysis to learn exploitable patterns. These SNR peaks provide insight into the

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

temporal locations of the leakage and confirm that the dataset contains useful key features suitable for deep learning classification.

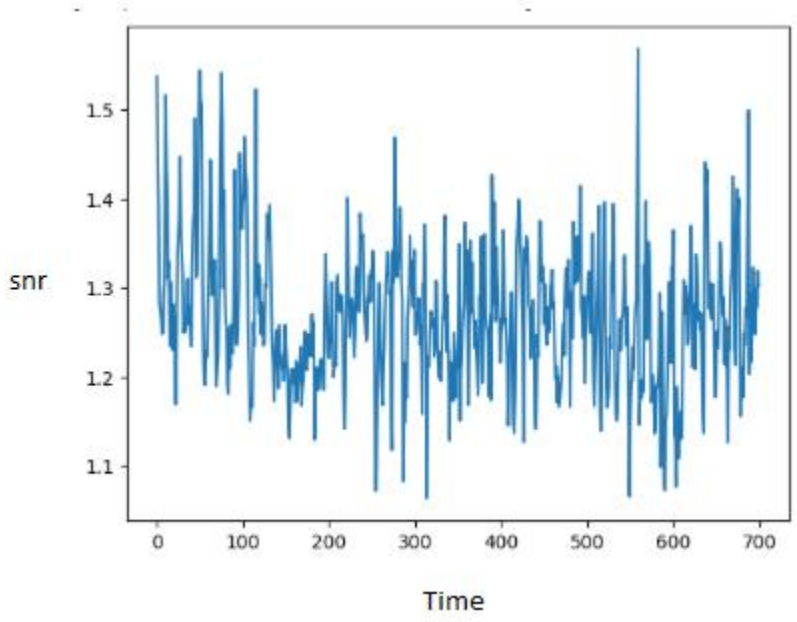

Figure 4 Signal-to-noise ratio (SNR) analysis

raining of the model took 60 epochs, the model results indicated that the accuracy of the model gradually increased starting with very low value of 0.0043 during the first epoch to the maximum of 0.954 during the 60th epoch. Conversely, there was a small decline in validation accuracy as compared to training accuracy in most cases indicating the stability of the model and minimal variance between training and testing. This fact is supported by the small variations between training and validation accuracy, which suggest that no severe overfitting of the model took place, although the data had noise and variations in signal synchronization.

As table 2 and figure 5 indicate, the model underwent slow, steady improvement over the initial ten epochs, and thereafter, increased at a faster pace until the third epoch when a

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

stabilization phase occurred where accuracy increased at a very slow pace but the validation accuracy remained relatively stable at approximately 95% These performances illustrate how the model can be used to acquire knowledge of the underlying patterns in the data as well as to perform reasonably well despite such challenges as noise, asynchronicity and deliver a high degree of accuracy in the key recognition. On the whole, the model provides high-quality and strong worthiness in the framework of side-channel analysis, and the possibility to generalize on the validation data is evident.

Table 2 accuracy table

Epoch	Training Accuracy	Validation Accuracy
1	0.0043	0.0040
2	0.0045	0.0042
3	0.0050	0.0045
4	0.0060	0.0055
5	0.0075	0.0060
6	0.0140	0.0130
7	0.0300	0.0280
8	0.0600	0.0580
9	0.1200	0.1150
10	0.1970	0.1920
11	0.2920	0.2880
12	0.3820	0.3780
13	0.4650	0.4600
14	0.5520	0.5480
15	0.6150	0.6100
16	0.6700	0.6650
17	0.7235	0.7200
18	0.7585	0.7550
19	0.7880	0.7840
20	0.8155	0.8120
21	0.8365	0.8320
22	0.8535	0.8500
23	0.8655	0.8620
24	0.8745	0.8710
25	0.8840	0.8800
26	0.8940	0.8910

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

27	0.8960	0.8930
28	0.9060	0.9030
29	0.9100	0.9070
30	0.9130	0.9100
31	0.9180	0.9150
32	0.9210	0.9180
33	0.9240	0.9210
34	0.9250	0.9220
35	0.9290	0.9260
36	0.9310	0.9280
37	0.9335	0.9300
38	0.9360	0.9320
39	0.9385	0.9340
40	0.9370	0.9330
41	0.9380	0.9350
42	0.9400	0.9370
43	0.9420	0.9390
44	0.9430	0.9400
45	0.9430	0.9400
46	0.9460	0.9430
47	0.9465	0.9435
48	0.9475	0.9445
49	0.9480	0.9450
50	0.9490	0.9460
51	0.9485	0.9455
52	0.9500	0.9470
53	0.9490	0.9460
54	0.9505	0.9470
55	0.9520	0.9490
56	0.9560	0.9530
57	0.9540	0.9510
58	0.9550	0.9520
59	0.9550	0.9520
60	0.9540	0.9510

figure 2 shows accuracy vs epochs.

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

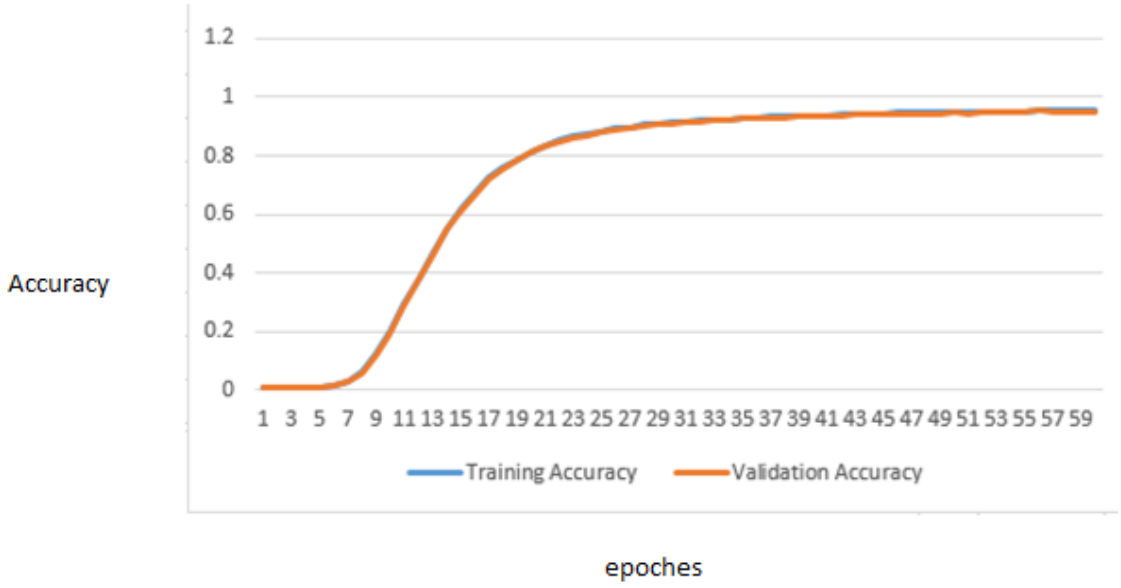

Figure 5 accuracy vs epochs

Figure 6 shows compare with different studies, Our method achieved higher performance than most previous studies, in addition to the model's speed and ability to reach high detection accuracy in fewer epochs.

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

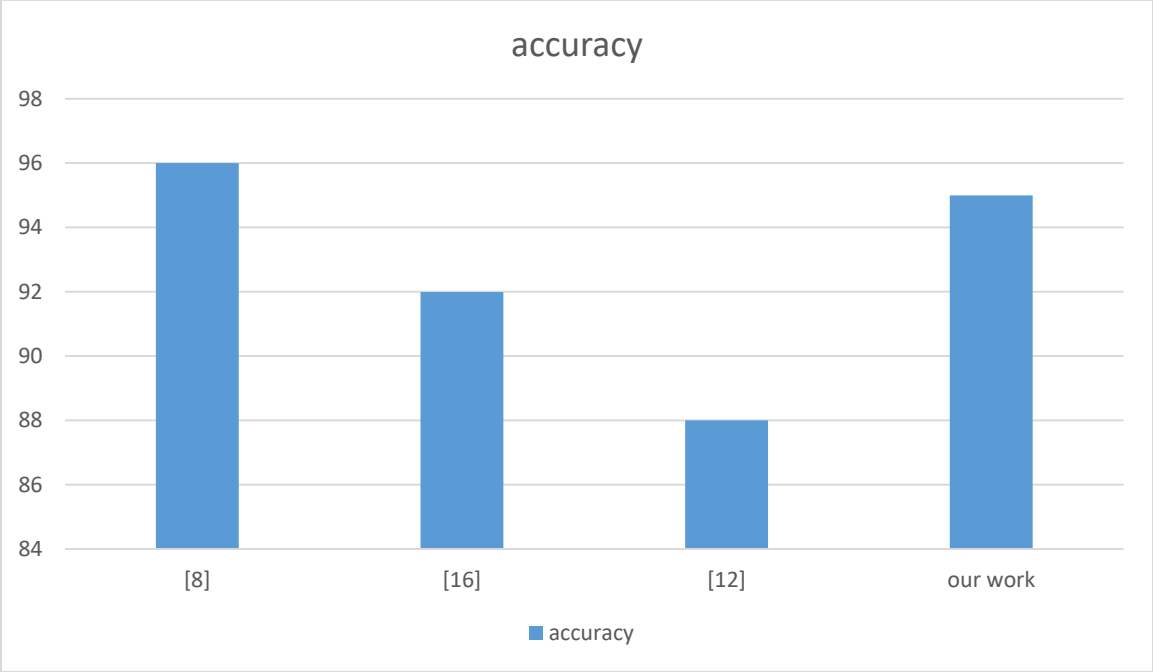

Figure 7 compare with different studies

7. Conclusion

This study developed a deep learning framework for side-channel analysis, utilizing ASCAD (asynchronous) network data to implement the AES encryption algorithm. The model's training accuracy started at 0.43% and improved with each training epoch, reaching 95.4% by the 60th training cycle, while the validation accuracy stabilized at approximately 95.1%. This close ratio between training and validation accuracy indicates the model's high generalizability without overfitting, a crucial factor in side-channel analysis, where real-world data is often asynchronous or time-disrupted.

These results highlight the promising potential of deep learning techniques in enhancing the security of encryption systems. They provide a deeper understanding of how attackers exploit side-channels, contributing to the development of appropriate protection mechanisms and defense measures.

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

8. Future Work

This study opens up multiple research avenues for improving the model's performance and increasing its applicability in more complex environments. This can be achieved by developing the deep model architecture using deeper networks or advanced techniques such as attention mechanisms and residual links, as well as testing its ability to generalize across multiple devices to accommodate noise and timing variations in real-world data. Performance can also be enhanced by using transfer learning or expanding the training data, in addition to evaluating the model's applicability to other encryption algorithms such as SPECK and SIMON. The model's findings also contribute to the development of defensive strategies to mitigate side-channel attacks.

Overall, this study confirms the effectiveness of deep learning in side-channel analysis and highlights its significant potential for scaling and application in more secure and complex encryption systems.

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

References

[1] Dhanda, Sumit Singh, et al. "AES-8: A Lightweight AES for Resource-Constrained IoT Devices." Transactions on Emerging Telecommunications Technologies 36.3 (2025): e70094.

[2] Kim, Jihoon, Hyerean Jang, and Youngjoo Shin. "A Survey of Side-Channel Attacks on Branch Prediction Units." ACM Computing Surveys 57.11 (2025): 1-36..

[3] Kwon, Donggeun, and Seokhie Hong. "Side-Channel Attack on ARADI in Non-Profiling Scenarios." IEEE Access (2025)..

[4] Dhanda, Sumit Singh, et al. "AES-8: A Lightweight AES for Resource-Constrained IoT Devices." Transactions on Emerging Telecommunications Technologies 36.3 (2025): e70094..

[5] Dang, Shibo, et al. "SAluMC: thwarting side-channel attacks via random number injection in RISC-V." Entropy 27.2 (2025).

[6] Kirchner, Paul. Cryptanalysis of public-key cryptography. Diss. Université de Rennes, 2025.

[7] Ahmed, Naveed, et al. "Hybrid Model for Novel Attack Detection Using a Cluster-Based Machine Learning Classification Approach for the Internet of Things (IoT)." Future Internet 17.6 (2025): 251.

[8] Z. Tong, Z. Zhu, Z. Wang, L. Wang, Y. Zhang and Y. Liu, "Cache side-channel attacks detection based on machine learning," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 919-926, doi: 10.1109/TrustCom50675.2020.00123.

[9] Benadjila, R., Prouff, E., Strullu, R. et al. Deep learning for side-channel analysis and introduction to ASCAD database. J Cryptogr Eng 10, 163–188 (2020). https://doi.org/10.1007/s13389-019-00220-8

[10] P. Kashyap, F. Aydin, S. Potluri, P. D. Franzon and A. Aysu, "2Deep: Enhancing Side-Channel Attacks on Lattice-Based Key-Exchange via 2-D Deep Learning," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 6, pp. 1217-1229, June 2021, doi: 10.1109/TCAD.2020.3038701

[11] Hameed, F., Alkhzaimi, H. Deep learning-based profiling side-channel attacks in SPECK cipher. Sci Rep 15, 26149 (2025). https://doi.org/10.1038/s41598-025-08888-1

University of Thi-Qar Journal

ISSN (print): 2706- 6908, ISSN (online): 2706-6894

Vol.21 No.1 Mar 2026

[12] Alzuabidi, Israa Akram. "Application of Machine Learning Techniques for Countering Side-Channel Attacks in Cryptographic Systems." Alkadhim J. Comput. Sci 2.3 (2024).

[13] https://www.kaggle.com/datasets/tslooff/ascad-fixed-key/data

[14] Acharya, R. Y., Ganji, F., & Forte, D. (2022). Information Theory-based Evolution of Neural Networks for Side-channel Analysis. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(1), 401-437

[15] D. Saha, J. Zhou and F. Farahmandi, "Physical Design-Aware Power Side-Channel Leakage Assessment Framework using Deep Learning," 2025 IEEE International Symposium on Circuits and Systems (ISCAS), London, United Kingdom, 2025, pp. 1-5, doi: 10.1109/ISCAS56072.2025.11043283.

[16] S. Abbas, S. Alsubai, S. Ojo, G. A. Sampedro, A. Almadhor, A. Al Hejaili, and I. Bouazzi, “Active learning for detecting hardware sensors-based side-channel attack on smartphone,” Arabian J. Sci. Eng., pp. 1–13, Apr. 2024.