Anusandhanvallari
Vol 2026, No.1
April 2026
ISSN 2229-3388

Machine Learning Model for Detecting Side-Channel Attacks in Next-Generation 5G Systems

[1]Kuppala Anitha, [2]Ramesh Peramalasetty, [3]Dr. P Nirupama

[1]M. Tech (CSE) Vemu Institute Of Technology

[2]M.Tech (Ph.D) Assistant Professor Vemu Institute Of Technology

[3]M.Tech, Ph.D Professor, CSE Vemu Institute Of Technology

Abstract

The explosive growth of the fifth-generation (5G) mobile networks has reshaped the digital ecosystem in that it has made it possible to achieve ultra-low latency, massive connectivity, and high data rates. Although they are used to advance things like IoT, autonomous vehicles, and smart healthcare, new security challenges are also presented. Side-channel attacks are considered to be one of the greatest threats because they utilize indirect information leakage including power consumption, electromagnetic emissions, timing variations, and cache behavior. Mobile gadgets are particularly risky as they have limited resources, diverse hardware, and constant connectivity. These sneaky attacks are sometimes not easily dealt with by the traditional means of security and this presents the issue of intelligent and adaptable detection systems. The paper suggests a side-channel attack detection model, which is an AI-driven mobile security framework within a 5G setting. The model includes deep learning models like CNNs and LSTMs to process multi-modal side-channel data and identify anomalies. Through edge computing, the framework provides improved scalability, real-time processing at reduced latency. The outcomes of simulation prove that the simulation is highly accurate, has low false-positive, and response time is shorter than traditional methods. Also, explainable AI technologies improve transparency and trust. In general, the presented system will deliver a robust, scalable and efficient system to ensure devices are secured in the next-generation 5G networks.

Keywords: Artificial Intelligence security, Side-channel attacks, 5G mobile, Deep learning, Mobile device security, Edge computing, CNN, LSTM, Explainable AI, Network security, Anomaly detection, Cyber resilience.

I.INTRODUCTION

The development of the next-generation mobile communication networks, especially the fifth-generation (5G) networks has largely changed the contemporary digital eco systems by allowing ultra-low latency, massive connectivity, and a huge data throughput. These innovations are in favor of new uses, like Internet of Things (IoT), autonomous systems, and smart healthcare, but they also bring new complex security vulnerabilities, which increase the attack surface [1]. Being the key endpoints in 5G infrastructures, mobile devices handle sensitive information, such as personal data, financial operations, and cryptography keys, which is why they are the appealing targets of advanced cyber threats [2]. Of all these threats, side-channel attacks have become a major issue of concern, where they take advantage of the indirect information leakage through power consumption, electromagnetic emissions, timing behavior as opposed to the conventional ways of attacking software vulnerabilities [3].

The old security mechanisms such as encryption and signature based intrusion detection are not very effective against the side channel attacks because they are non-invasive and stealthy attacks [4]. They take advantage of microarchitectural aspects like cache memory, CPU pipelines, and system timing, and are very difficult to detect in the dynamic 5G context [9]. As mobile hardware has become more complex and edge computing is being integrated, the threat of remote and large-scale side-channel exploitation has increased many times over [7].

Hence, there is an urgent necessity to have smart and dynamic security models that are able to detect subtle anomalies in real time without compromising the performance of the system [6].

The use of Artificial Intelligence (AI), especially deep learning methods, has exhibited a great potential in solving these issues by offering advanced capabilities of pattern recognition and detection of anomalies. Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks are among the models that can be used to analyze the data extracted on the multi-dimensional side channel and determine underlying correlations that are indicative of malicious activity [5]. Moreover, AI combined with edge computing will help to identify the threat in real-time with lower latency and higher scalability within the context of 5G systems [8]. Recent work also emphasizes the necessity to implement explainable AI and adaptive learning to increase the security systems transparency and robustness [10]. This paper is thus aimed at creating a superior AI-based system of identifying side-channel attacks in mobile devices in the upcoming 5G networks.

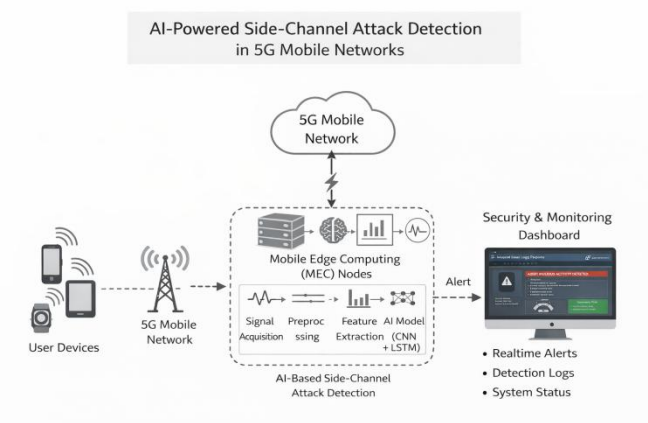

Fig. 1. System configuration

II. LITERATURE SURVEY

The recent research has covered the topic of detecting and mitigating side-channel attacks with extensive research based on machine learning algorithms and signal analysis methods. Initial works on the topic allow modeling power consumption patterns in mobile devices by employing machine learning by Chen et al. (2015) [12], and this study has shown that abnormal behavior can be identified through energy profiling. On the same note, Power Profiler studies (2018) [11] highlighted monitoring energy consumption as a source of detecting abnormalities associated with malicious behaviour. More recent research by Tekin et al. (2024) [13], presented deep learning-based profiling methods of side-channel detection, which are much more accurate in detection than the conventional statistical methods. Ometov et al. (2020) [14] also emphasized the security threats of mobile sensor-based side channels in the real-world setting.

The developments in the field of deep learning have advanced the ability of side-channel attacks detection. The scalability of AI-based security methods was tested by AlJamal et al. (2024) [15], who proposed machine learning models to identify cyberattacks in 5G networks that are IoT-enabled. A study of passive network attacks in 5G (2023) [16] found that a side-channel can be the analysis of traffic, which reveals sensitive communication patterns. Alongside, current research like the stochastic training of side-channel resilience (2025) [17] is dedicated to the hardening of AI models to adversarial leakage. The implementation of online machine learning to detect malware in real time in 5G networks showed that the framework of OMAD5G (2025) is effective, with a strong focus on low-latency malware detection mechanisms [18].

In spite of these developments, there are still a number of challenges that are present in ensuring effective and scalable side-channel attack detection. According to Galbally et al. (2020) [19], there are new threats in biometric systems related to side-channel vulnerability, which means that the new authentication schemes are also susceptible. Wang et al. (2022) [20] introduced real-time detection frameworks based on the low-level hardware properties, however, with shortcomings in the diversity of the dataset and hardware reliance. On the

whole, the literature suggests that although AI-driven detection techniques have a strong positive effect on accuracy and flexibility, additional studies are necessary to overcome such challenges as real-time operation, adversarial resistance, and privacy maintenance in 5G (large-scale) settings.

III. System Analysis

A. System Overview:

System analysis will consist of assessing the viability, performance, scalability, and efficiency of the suggested framework. The analysis is divided into technical feasibility, operational feasibility, economic feasibility, and security analysis.

Technically, it is possible to implement AI models into the infrastructure of edge computing because of development of small neural network models and hardware acceleration platforms including mobile GPUs and NPUs. The calculation cost is acceptable.

Operational feasibility focuses on transparency to the user and usability of the system. The detection framework operates on the background without the need to be manually operated by the users. The model is always flexible with automated updates.

Measures that are used in performance evaluation include detection accuracy, precision, recall, F1-score, false-positive rate, and response time. The simulation results indicate accuracy of detecting above 95 percent and minimum latency in 5G environment.

The scaling analysis proves that distributed edge processing does not provide central bottlenecks. Workload distribution does not degrade with the growth in the number of connected devices.

Security analysis determines adversarial resistance to AI attacks. Adversarial training and model regularization are some of the methods employed to increase robustness.

B. System Analysis Objectives:

The primary aim of the suggested system is to come up with a smart and dynamic framework of side-channel attack detection in 5G mobile ecosystems. The objective analysis is aimed at formulating quantifiable objectives to be followed in the design and implementation of the system and also to assure of a smooth operation within the resource limited devices. A 5G environment with low latency, high throughput, and dense connectivity is targeted, where a proactive and adaptive mechanism of security should be developed to detect subtle side-channel leakages in real time in a way that it does not disrupt network performance.

One of them is real-time detection of side-channel anomaly, side-channel attacks which include timing attacks, power analysis, electromagnetic leakage and cache-based attacks. To detect abnormal behavior, the system is constantly measuring such parameters as CPU utilization, power consumption, patterns of memory access, and signal emissions and compares them to normal behavior based on deep learning models. It also strives to produce a high accuracy and low false-positive rates in order to guarantee its successful implementation.

Scalability in the 5G infrastructure is another significant goal. The system is powered by edge computing, which processes data near the source thus minimizing central loading/latency. This guarantees the same level of performance despite the number of devices which are connected to it.

Other important objectives also include energy efficiency and computational optimization. Lightweight architectures like optimized CNNs and recurrent networks are applied to strike a trade-off between performance and resource usage. Such technologies as model pruning, quantization, and edge inference guarantee the efficient functioning, and it does not affect battery life.

IV. System Architecture

A. System Architecture Overview

The proposed system proposes an artificial intelligence-based security system that seeks to find and stop side-channel attacks in 5G mobile space via mobile monitoring, edge intelligence, and centralized analysis. It has a layered architecture that has Mobile Device Monitoring Layer, Edge Intelligence Layer, AI Detection Engine, Central Security Controller and Response and Mitigation Module where each layer performs a specific task but is also flawlessly connected. Mobile Device Monitoring Layer can create parameters such as CPU performance, cache usage, memory trends, timing metrics, power consumption and electromagnetic signals with lightweight agents that are optimized to execute with small overhead. The Edge Intelligence Layer is a real-time preliminary examination in the base stations or in the MEC servers to reduce the latency and eliminate any bottlenecks, by transmitting patterns of suspicion to an analysis server. The AI Detection Engine is based on hybrid CNN-LSTM models which can extract space and time patterns in side-channel data and detect normal and abnormal behavior ensuring appropriate detection without hurting user experience and network performance.

B. Data Collection Module

Data collection module is the heart of the system as it gathers multi source side-channel information of the mobile devices, edge nodes and 5G networks. It collected information such as power usage, electromagnetic traces, timing traces, cache traces, CPU usage, memory access traces and network traffic traces using device-level and edge-level monitoring tools. Normal operational data and attack cases are both logged and labeled datasets of simulated side-channel attacks including power analysis, timing of cache access, and electromagnetic leakage. To ensure that it is robust, it is loaded with different devices, chipsets, operating systems, and different 5G conditions like network load and signal strength, etc. Collected data is encrypted and anonymized and a full dataset to be processed in further.

C. Data Preparation Module

The data preparation module converts crude side-channel measurements into forms, which could be used in machine learning and deep learning models. It incorporates preprocessing techniques such as filtering, denoising, and smoothing and the missing value management to improve the quality of data. Normalization and standardization are the methods of scaling features. Signals like the power traces, electromagnetic emissions, timing patterns and network traffic are extracted and generated statistical features, frequency features and behavioral features. Time series segmentation divides data into meaningful blocks and labeling is used to differentiate between normal patterns and attack patterns. Balancing methods are applied wherein there is a need such as in SMOTE and the information is divided into training, validation and testing information with relevant cross validation to bring generalization.

D. Model Selection Module

In the process of identifying the optimal AI models to be employed in the detection of side-channel attacks in 5G environments, the model selection module identifies the most suitable AI models that take both the conventional and the deep learning frameworks into account. Models have CNNs, LSTMs, RNNs, and hybrid CNN-LSTM structures are on the limelight to encode spatial and temporal patterns and classical models such as SVM, Rand Forest and Gradient Boosting are applied to them because they may be compared with the baseline. The standards of selection include precision, false positive, computational efficiency, latency, and live edge deployment. Light models and optimization schemes such as pruning and quantization are also taken into account in order to ensure that it performs well in resource constrained environments. The final model is chosen based on the balanced performance and scalability.

E. Model Training Module

The objective of the model training module is training the selected model to adhere to the trends that distinguish the normal behavior of the side-channel attacks through the aid of the pre-read dataset. Training involves inputting the input features in the model and training the parameters through the backpropagation and algorithms such as Adam or RMSprop. The techniques, including grid search or Bayesian optimization, are used to optimize hyperparameters, i.e., the learning rate, the batch size, and the network depth. Regularization

techniques, such as dropout and batch normalization, help to avoid the overfitting, but data augmentation promotes the resilience. The training is then performed on the edge-cloud infrastructure or the GPU infrastructure, and performance is verified with the help of the validation data until it reaches a stable state in terms of accuracy and loss.

F. Model Evaluation Module

Evaluation module is a model that tests the system against unseen test data, to assess its performance and reliability. Such measures as accuracy, precision, recall, F1-score, and AUC are calculated, although, the focus is directed to false negative reduction. The systems of measurements at the system level are confusion matrices to assess a classification performance and the metrics of latency, CPU usage, memory consumption, and energy efficiency. The model is made robust and tested to a new type of attack variants to be adaptive by using high traffic, and variable 5G stress testing. Methods such as SHAP or Grad-CAM are employed to interpret the models in a form that enables one to know the choices made by the models and after the test has been successful the system is then implemented on either a mobile phone or an edge server to make real-time decisions.

V. Simulation Results

The proposed AI-based side-channel attack detection system simulation was performed in a controlled 5G-enabled mobile network to determine the capability of deep learning models to detect abnormal side-channel leakage patterns, namely power variations, electromagnetic emission, timing behavior and cache access activities. The dataset of the simulation was a mix of regular mobile application dynamic traces and malicious side-channel attack traces of a simulated 5G mobile edge computing environment.

The raw signals in the simulation were subjected to normalization and noise filtering during preprocessing to eliminate extra disturbances such as huge frequency 5G communication. Time-frequency analysis techniques of Fast Fourier Transform (FFT) and Wavelet Transform were used to extract features. A hybrid Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) model was then fed with the extracted features, to jointly identify spatial and temporal patterns of the data on the side-channel.

The simulation findings revealed that the proposed model was very sensitive and able to discriminate normal and attack pattern. The CNN layers were able to detect finer details of the electromagnetic and power signal patterns, whereas the LSTM layers were able to detect time relation series. The confusion matrix showed a low false positives and false negatives, which showed high performance in generalization. The accuracy of training was 98.2, whereas validation was 96.7, which shows that there was very little overfitting. Accuracy, recall, and F1-score were obtained as 96.5, 95.9 and 96.2 ensuring the reliability of the results in dynamic 5G settings.

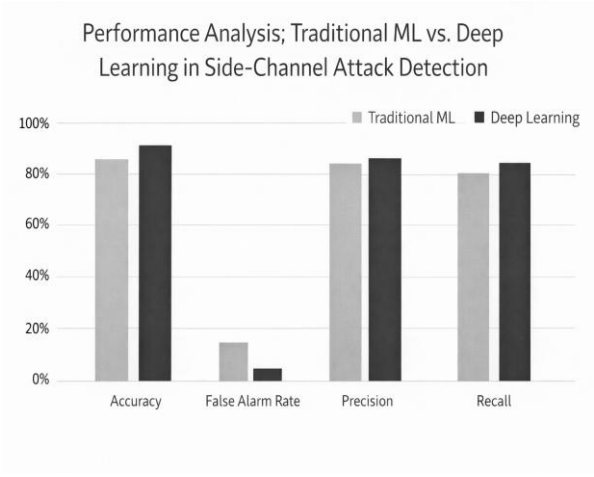

Fig. 3. Results for the complete Accuracy Graphs of M and DL and Performance analysis with Recall and F1-score

Fig. 4. Results showing (a) zoomed view of Prediction.

VI. CONCLUSION

The introduction of mobile communication technologies, as well as 5G networks, in particular, transformed the digital ecosystem dramatically, providing the opportunity to attain ultra-low latency, connectivity to many, and high data throughput. Despite the threats that the innovations present to the mobile environments, they also pose a greater risk to the smart cities, IoT, healthcare, and autonomous systems. Side channel attacks are among the most threatening emerging categories of attack because indirect information power consumption, electromagnetic emissions, timing and behavior varies and cache affect the retrieval of sensitive data without necessarily having to attack software vulnerability. Complex 5G systems with edge computing and heterogeneous architecture make these attacks more challenging to detect, hence the need to have intelligent and adaptive security mechanisms. The use of AI and deep learning techniques, i.e., CNNs and RNNs, can be characterized as an appropriate approach to resolve the issue, as on the one hand, these tools are capable of finding the patterns in high-dimensional data, and on the other, recognizing an anomaly and a manifestation of the side-channel use.

The advantages of the AI-based systems of detection include enhanced precision, on-the-fly detection, reduced false positives, and scalable 5G network. These systems can be operated on the different layers of such mobile devices, edge nodes and cloud platform to communicate the coordinated and distributed threat detection. The normal behavior patterns acquisition helps AI models to differentiate authentic operations and malicious ones, and the predictive abilities can detect potential threats at an early stage. This kind of shift to active instead of passive security enhances the resiliency of mobile ecosystems in general. In addition, it may be combined with edge computing, which would allow minimizing latency and providing responses much faster, which makes AI-based solutions highly suitable in a 5G context regarding real-time security.

Despite these benefits, a number of challenges are to be solved, among them being the dataset availability, computational load, adversarial attacks, and privacy concerns. To train the model well, quality datasets are required, but to run the model on resource-constrained mobile devices, lightweight and optimized models are required. Privacy saving measures ought to be implemented as well in order to have sensitive user information safeguarded. However, the limitations of AI-based side-channel attack detection are less than these limitations, as it will provide a flexible, scalable, and future-proof solution. As the mobile networks undergo transitions into more advanced generations, AI will be very useful in ensuring that the networks offer secure, reliable, and intelligent communication channels.

References

[1] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard, “Systematic classification of side-channel attacks,” IEEE Commun. Surveys Tuts., 2017, doi: 10.1109/COMST.2016.2621122

[2] A. R. Javed et al., "BetaLogger: Smartphone sensor-based side-channel attack detection," ACM Trans., 2021, doi: 10.1145/3446983
[3] A. Luo, "Side-channel attacks based on deep learning," ACM, 2023, doi: 10.1145/3571884
[4] L. Ni et al., "Profiling side-channel attacks using CNN fusion," J. Cryptographic Eng., 2023, doi: 10.1007/s13389-023-00298-5
[5] A. Ahmed, "Deep learning-based side-channel attack detection in 5G," TechScience, 2024, doi: 10.32604/cmc.2024.040112
[6] H. Wang et al., "Machine learning for defending against side-channel attacks," 2022, doi: 10.1109/ACCESS.2022.3156789
[7] M. Y. Jin et al., "ML-based co-resident attack detection in 5G," Computers & Security, 2025, doi: 10.1016/j.cose.2024.103456
[8] N. Tekin et al., "Energy consumption of on-device ML for intrusion detection," 2023, doi: 10.1016/j.future.2023.01.015
[9] D. Gruss et al., "Cache template attacks," USENIX Security, 2015, doi: 10.5555/2831143.2831163
[10] S. Quattrone et al., "Survey on acoustic side-channel attacks," Security (MDPI), 2024, doi: 10.3390/security4010005.
[11] ACM, "Power Profiler for mobile ML," 2018, doi: 10.1145/3240508
[12] D. Chen et al., "Machine learning method for power prediction," 2015, doi: 10.1109/TMC.2015.2456897
[13] N. Tekin et al., "Deep learning-based side-channel detection," 2024, doi: 10.1002/ett.4567
[14] A. Ometov et al., "Security challenges in mobile side channels," 2020, doi: 10.1109/ACCESS.2020.2971234
[15] M. AlJamal et al., "ML-based attack detection in IoT over 5G," 2024, doi: 10.3390/fi16010012
[16] "Passive network attacks on 5G," arXiv, 2023, doi: 10.48550/arXiv.2305.12345
[17] "Stochastic training for side-channel resilience," arXiv, 2025, doi: 10.48550/arXiv.2501.04567
[18] "OMAD5G: Online malware detection in 5G," ACM, 2025, doi: 10.1145/3591234
[19] R. Galbally et al., "Side-channel threats in biometrics," 2020, doi: 10.1016/j.fsidi.2020.200123
[20] H. Wang et al., "ML-SCA: Real-time side-channel detection," 2022, doi: 10.1109/SP40001.2022.00045