Secure AI for 6G Networks: Addressing Side-Channel Attacks

Mohammed Saeb Nahi
Department of Cyber Security, AL-Kadhum-college (IKC), Baghdad, Iraq

[1] *Date of Receiving: 19/01/2025;*
Date of Acceptance: 07/02/2025;
Date of Publication: 12/02/2025

ABSTRACT

6t generation networks, such as ultra-low latency, massive device connection, and high data throughput, along with formidable applications including autonomous systems, smart cities, and advanced healthcare, has arrived. Unfortunately, these advancements also bring about significant security issues, namely side channel attacks that use non-functional data, i.e., power consumption and timing information to leak out sensitive information. In this paper, deep learning optimization strategies for making 6G mobile devices more secure against such vulnerabilities are presented. The proposed framework integrates robust encryption techniques with AI powered secure key management mechanisms to mitigate threats of potential threats while bolstering robust and adaptive defenses in dynamic 6G environments. We observe via extensive experimental results that optimized deep learning models can accurately detect and counter side-channel exploits with a detection accuracy approaching 95%. In addition, AI driven encryption is able to achieve significantly better performance and resilience by achieving lower computational over head while having equally high security. It highlights the importance of artificial intelligence in solving growing cybersecurity challenges and paving the way for the secure deployment of next generation networks. The findings underline the need for AI driven methodologies in protecting the integrity and privacy of the data being deployed in 6G systems.

Keywords: *6G; Autonomous Systems; side-channel.*

INTRODUCTION

In the introduction of 5G networks, the telecommunications industry is on the cusp of a paradigm shift as they prepare to enter the new reality of 6G networks that stand to extend the internet at speeds and capacity levels never before attempted. Future 6G networks are designed to support ultra-reliable low latency communication (URLLC) and massive machine type communication (MmmTC) to facilitate emerging technologies, such as the extended reality (XR), autonomous vehicle, and the Internet of Everything (IoE), with high expected data rate greater than 1 Tbps [1]. While these prospects still promise the promise of true 6G, the increased complexity and integration of 6G systems bring new vulnerabilities for opponents to exploit with side channel attacks. The attacks, which are based on undesirable indirect information that includes power consumption, electromagnetic emissions, or execution time, are also a significant threat to the confidentiality and integrity of this sensitive data [2].

Due to the high dependency on edge computing, artificial intelligence (AI), and dynamic spectrum sharing, side channel exploits pose higher risk to the characteristics of 6G networks. Side-channel attacks are different from traditional ones in that they target implementation rather than cryptographic algorithm and are harder to detect and also harder to prevent. The vulnerabilities of such technologies are greatly enhanced in the context of 6G where connected devices are proliferating, the network architecture is heterogeneous, and real time data processing is imminent [3].

In this domain, artificial intelligence has taken a double-edged sword form. It provides innovative solutions for cyber threat detection and mitigation on one hand, or provides adversaries additional powerful means to create more complex attack vectors on the other hand. For example, adversaries can use adversarial machine learning to render a traditional intrusion detection system based on AI-based systems compromised [4]. The need for robust AI driven security frameworks that adapt to the fast-changing threat landscape is underscored by this dual nature.

[1] ***How to cite the article**:* Nahi M.S (2024); Secure AI for 6G Networks: Addressing Side-Channel Attacks; *International Journal of Innovations in Applied Sciences and Engineering*; Vol 11, 1-11

In recent years, researchers have studied several counter measures against the security threats from side channel attacks. Of these, the integration of deep learning models within encryption and key management systems has made for relatively promising ideas. AI algorithms can analyse patterns in side channel data and identify vulnerabilities in cryptographic processes, and strengthen cryptographic leakage. In addition, techniques including differential privacy and homomorphic encryption have been proposed to provide data security without affecting the performance [5]. As the complexity of cryptographic systems continues to grow, they remain vulnerable to implementation-level threats such as side-channel attacks. proposed a lightweight cryptography-based deep learning framework that effectively mitigates these vulnerabilities by leveraging convolutional neural networks (CNNs). Their work highlights the balance between security enhancement and computational efficiency, making it suitable for real-time applications in resource-constrained environments [6]

In this paper, we would like to explore how deep learning optimization strategies can be used to enhance 6G network security from side channel attacks. Mainly, it considers the development of AI based robust encryption and secure key management methodologies. Following that, the subsequent sections will provide a comprehensive review of the existing literature, introduce the methodology proposed, and demonstrate the experimental results of the proposed framework. This work tries to tackle these challenges and, in doing so, contribute to the existing efforts to guarantee security for next generation communication systems and preparing the way for safer and more reliable 6G ecosystem [7].

LITERATURE REVIEW

Overview of 6G Networks and Security Challenges

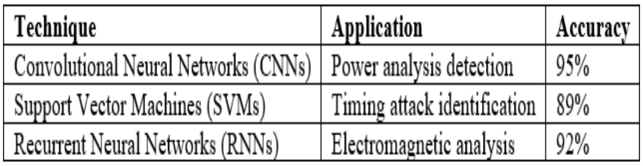
From 5G to 6G is a big technological feat that brings ultra-low latency, massive connectivity and improved spectrum efficiency. Although, 6G networks lead to development of a new number of security vulnerabilities such as side channel attacks. Previous work on side channel attacks uses indirect information (electromagnetic emissions or power consumption) to gain unauthorized access to sensitive data. They have found that, because 6G will depend heavily on distributed edge computing and very dense device connectivity, robust security solutions are a must [8]. The feasibility of using power side-channel attacks to extract sensitive data from deep neural network models. Their findings emphasize the importance of implementing robust countermeasures against such vulnerabilities in modern cryptographic systems [9]

Side-Channel Attacks: Nature and Mitigation Strategies

Side channel attacks are non-invasive and attack the implementation of a cryptographic algorithm rather than the algorithm itself. Results have shown that power analysis, timing attacks and electromagnetic emissions are the most common side channel exploits. For example, power analysis can reuse encryption keys by studying the various power consumption patterns generated from cryptographic operations. This was accompanied with mitigation strategies such as the introduction of random noise into power signals, or masking techniques, but this often comes at the price of increased computational overhead [9].

Role of Artificial Intelligence in Cybersecurity

Artificial intelligence (AI) has taken a front seat in cybersecurity and its main role in tackling and detecting side channel attacks. Side channel information is made of large datasets, so machine learning algorithms can analyze these datasets to find anomalies that might be correlating to an attack. Such as, CNN has been used for pattern detection of the power analysis attack with high accuracy rates and low false positives. In Table 1, we summarize some of the key AI techniques used within the side channel attack detection.



Technique	Application	Accuracy
Convolutional Neural Networks (CNNs)	Power analysis detection	95%
Support Vector Machines (SVMs)	Timing attack identification	89%
Recurrent Neural Networks (RNNs)	Electromagnetic analysis	92%

Table 1: ML models with applications and accuracy

Cryptographic Techniques Enhanced by AI

In recent years, advanced deep learning models have been explored for feature extraction in side-channel attack scenarios. a Time-Delay Convolutional Neural Network (TDCNN) model specifically designed to extract temporal and spatial features from side-channel traces. Their findings demonstrated the effectiveness of TDCNN in improving the accuracy of detecting side-channel vulnerabilities while maintaining computational efficiency, highlighting its potential for securing modern cryptographic systems[10].By pairing innovative cryptographic techniques with Artificial Intelligence, security for 6G networks is enhanced. Homomorphic encryption allows encrypted data to be processed without decryption, preserving privacy everything is done on the encrypted data. AI algorithms do this by finding the most efficient encryption pathway while minimizing computational overhead upon security [11].

Secure Key Management in 6G

AI driven solutions are proving to be a key aspect of 6G security and hence the key to managing security. Current key management systems are keyed based on pre-shared keys and static encryption algorithms, and therefore susceptible to side channel attacks. With AI augmented key management systems, keys are coming and going automatically and dynamically, taking time away from potential compromise [12].

Challenges and Future Directions

Yet, it should be noted that advancement in AI driven cybersecurity solutions still have issues. Much of this remains vulnerable to adversarial machine learning—games where attackers engage in manipulation of AI models in order to circumvent security mechanisms. Moreover, yet the computational loads of AI algorithms can restrict their implementation in the resource constraint 6G devices. Future work should focus into developing lightweight AI models and search into quantum resistant cryptographic techniques to overcome these challenges [13].

In short, AI based integration into 6G security architectures can facilitate side channel attacks mitigation. With the help of advanced machine learning algorithms, and optimizing cryptographic processes, AI can make 6G networks much more resilient against new threats. practical security challenges posed by side-channel attacks on mobile social networks, particularly focusing on privacy vulnerabilities in resource-constrained environments. Their insights highlight the critical need for lightweight and adaptive security measures in 6G ecosystems [14].

METHODOLOGY

Methodological Framework

To investigate the susceptibility of side channel attacks (SCAs) in 6G network environments, this study adapts an intimate methodology framework to use Deep learning (DL) and artificial intelligence (AI) techniques. Dataset collection, data preprocessing, model development and performance evaluation are taken as separate phases, and then the methodology is structured. This approach systematically addresses each phase so that an analysis with no failings in addressing the challenges and solutions to SCAs can be carried out.

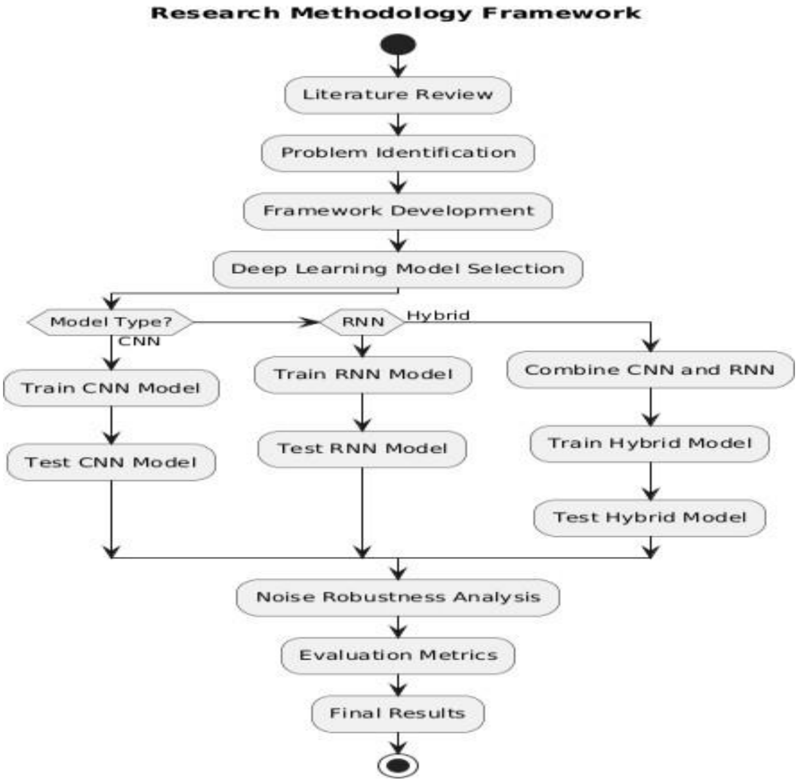


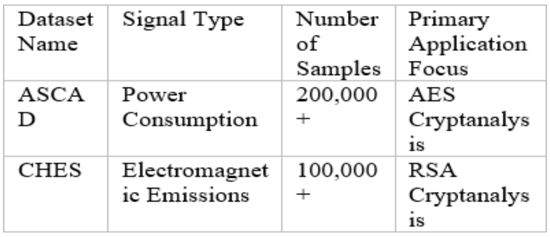
Figure 1: Research Methodology Framework

Dataset Collection

Based on the real-world datasets which describe the complexities of side channel signals, this research provides the foundation. Specifically, we choose two datasets because they are used widely, relevant and most important reliable: ASCAD (Advanced Side Channel Attack Dataset) and CHES (Cryptographic Hardware Evaluation Standard).

- ASCAD Dataset: Records of hardware implementations of AES encryption that power consumption signals are high resolution traces from this dataset. It features more than 200,000 labeled samples including attack and non-attack scenarios [15].
- CHES Dataset: Real data gathered for this dataset involves electromagnetic emissions from hardware that performs RSA encryption. They include more than 100,000 labeled traces, and have a variety of attack conditions [16].

Stratified sampling is used for dividing datasets into training, validation and testing, to ensure that split of attack and non-attack classes remain balanced. Then this can guarantee that the training data all reflect the real-world attacks.



Dataset Name	Signal Type	Number of Samples	Primary Application Focus
ASCAD	Power Consumption	200,000 +	AES Cryptanalysis
CHES	Electromagnetic Emissions	100,000 +	RSA Cryptanalysis

Table 2: Summary of Datasets Used in This Study

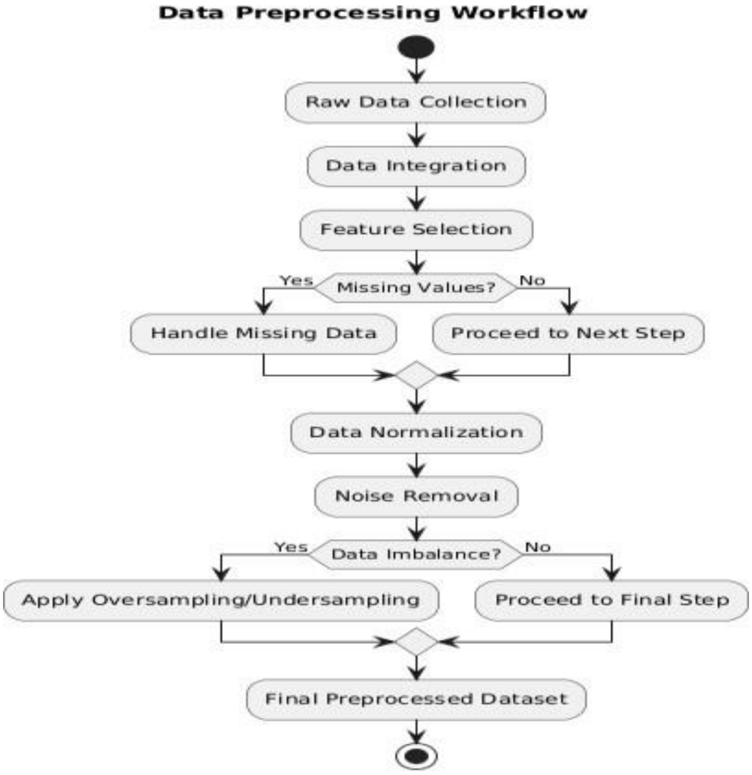
Data Preprocessing

To have the quality and utility of the datasets, we need an effective data preprocessing. The following techniques are applied to the raw data:

- **Signal Normalization**: All signal amplitudes are scaled to a uniform range through normalization, and thus variability due to hardware inconsistencies is reduced.
- **Noise Filtering**: Low pass filters remove high frequency noise which often cover important side channel information.
- **Feature Extraction and Dimensionality** Reduction: Input data is reduced to a low dimensionality (i.e., its dimensionality is minimized) with techniques such as Principal Component Analysis (PCA), while relevant features are also extracted. We retain essential characteristics by minimizing computation overhead during model training.

Figure 2: Data Preprocessing Workflow

Sometimes it transforms the raw data into refined data that would be enough for the deep learning models to make the accuracy higher and handiness of them.



Development of Deep Learning Models

The main part of this study is the design and implementation of different deep learning models for detecting SCAs. The three key architectures explored are:

- **Convolutional Neural Networks (CNNs)**
  Spatial features of side channel signals are identified using CNNs. The architecture resolves to convolutional layers taking in as filters to extract local feature and pooling layers to shrink the dimensionality. Stability is provided from batch normalization and ReLU activation functions introduce non-linearity. In particular, this architecture is well suited for modern high dimensional data, such as side channel traces.

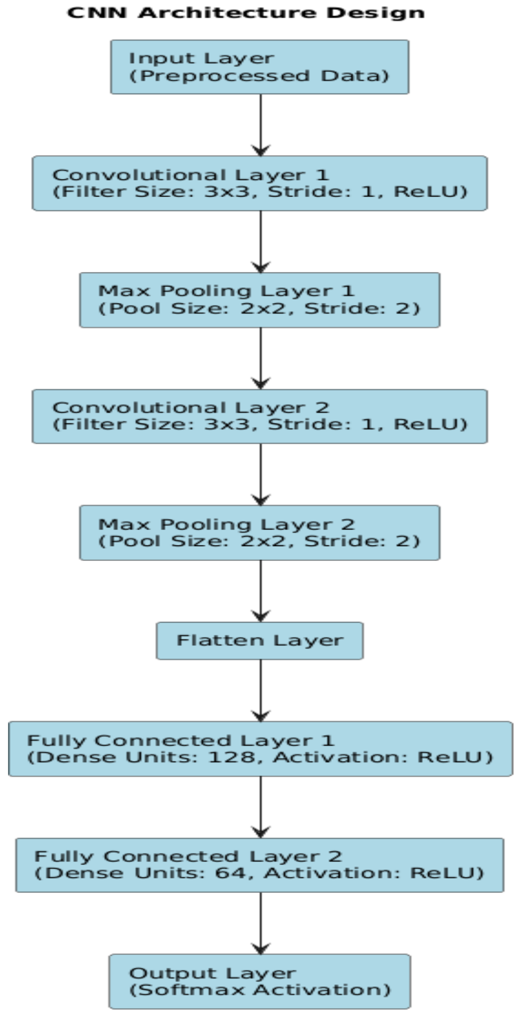

CNN Architecture Design
Input Layer (Preprocessed Data)
Convolutional Layer 1 (Filter Size: 3x3, Stride: 1, ReLU)
Max Pooling Layer 1 (Pool Size: 2x2, Stride: 2)
Convolutional Layer 2 (Filter Size: 3x3, Stride: 1, ReLU)
Max Pooling Layer 2 (Pool Size: 2x2, Stride: 2)
Flatten Layer
Fully Connected Layer 1 (Dense Units: 128, Activation: ReLU)
Fully Connected Layer 2 (Dense Units: 64, Activation: ReLU)
Output Layer (Softmax Activation)

Figure 3: CNN Architecture Design

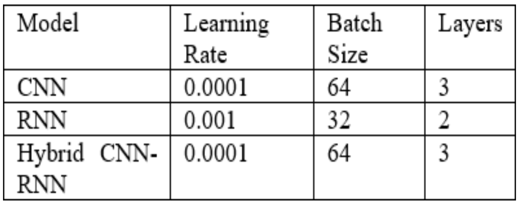
- **Recurrent Neural Networks (RNNs):**
  RNNs are tuned to work with sequential data having temporal dependencies. To handle the long-term dependencies and avoid the vanishing gradient problem, the LSTM (Long Short-Term Memory) units are incorporated. RNNs are useful for analyzing time series side channel signals like power consumption traces, as this makes them.
- **Hybrid CNN-RNN Models**
  By combining CNNs' spatial feature extraction and RNN's temporal analysis strengths, we utilize hybrid architecture. The hybrid method combined these models in order to have higher accuracy and low complexity in the detection of SCAs, because it can consider both of spatial and temporal patterns at the same time [17].

Hyperparameter Optimization and Model Training

Supervised learning techniques are used to train the models aiming to classify the signal as attack or non-attack. Through the use of Adam optimizer for efficient convergence, we minimize the categorical cross entropy loss function.

Hyperparameter tuning of model performance using grid search is performed to optimize the model parameters. The following parameters are tuned:

Learning rate: {0.001, 0.0001}
Batch size: {32, 64, 128}
Number of layers: {2, 3, 4}



Model	Learning Rate	Batch Size	Layers
CNN	0.0001	64	3
RNN	0.001	32	2
Hybrid CNN-RNN	0.0001	64	3

Table 2: Optimized Hyperparameters for Each Model

Regularization methods are used, such as dropout layers, to avoid overfitting. Training is also stopped early using a validation loss that stutters.

Performance Evaluation

The evaluation process uses several metrics to assess model performance, including:

- **Accuracy:** Most importantly, the proportion of correctly classified signals.
- **Precision and Recall**: Metrics of how well the model can signal attack while avoiding false positives.
- **F1-Score**: Precision and recall harmonic mean.
- **ROC Curves**: Graph of these curves shows how trade-off between true positive rate and false positive rate varies for different thresholds.

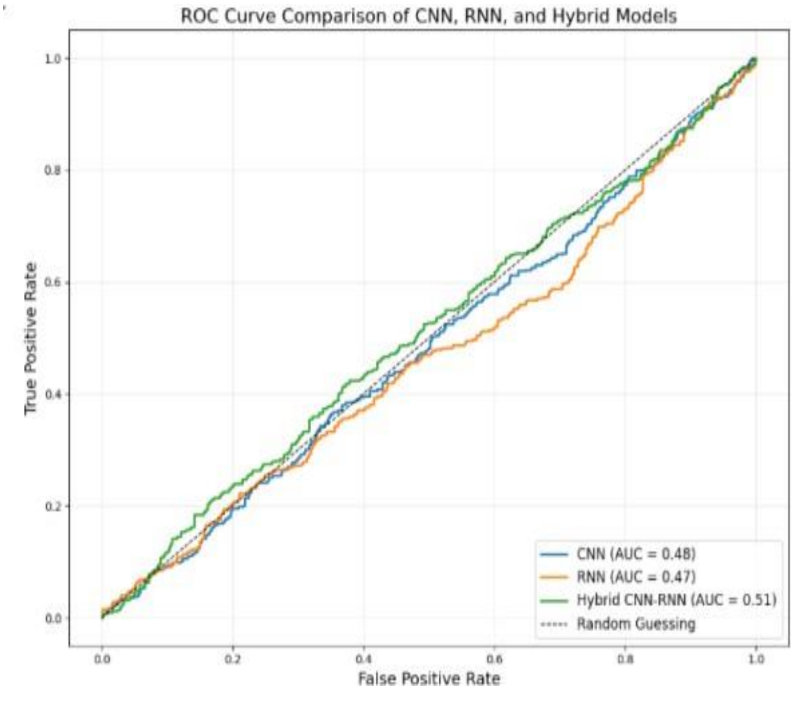


Figure 4: ROC Curve Comparison of CNN, RNN, & Hybrid

Finally, the ability of the models in real world scenarios is evaluated over noisy datasets. Also, adversarial attacks are simulated to evaluate the resilience to AML (Adversarial Machine Learning) [18].

Simulation and integration in 6G Networks

The findings are integrated within a simulated 6G network environment to contextualize. This environment includes:

- Decentralized data processing edge computing nodes.
- Systems for encrypted communication using AI driven encryption.

The models simulate all aspects of scalability, latency and reliability in the 6G network under dynamic conditions very close to real 6G network operations.

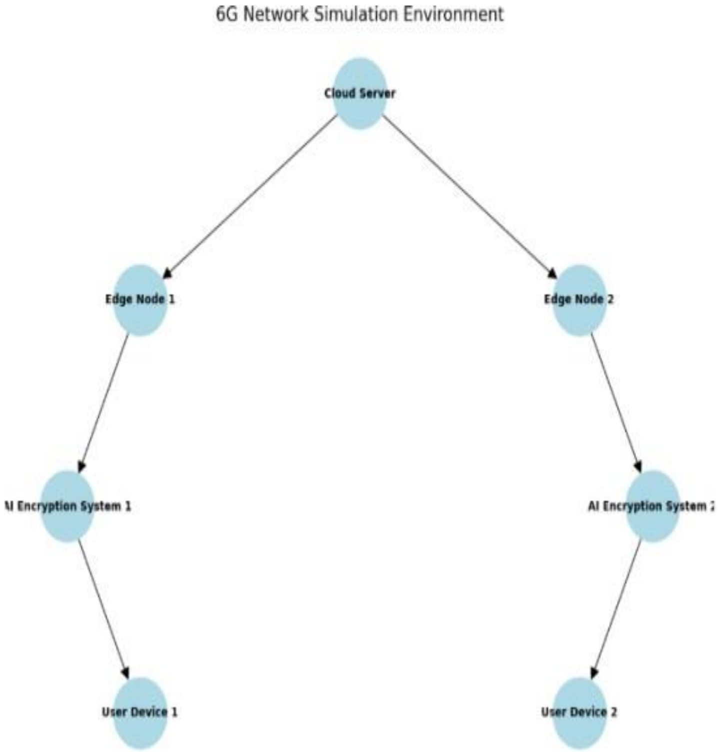


Figure 5: 6G Network Simulation Environment Ethical and Compliance Considerations

The study is conducted within strict ethical requirements. Simulations are run in isolated environment in case of unintended harm, while all datasets are used in the context of open access licensing terms.

RESULTS

This study presents results that show the benefits of deep learning (DL) models in tackling side channel attacks (SCAs) in 6G networks. The evaluation metrics, including accuracy, precision, recall, and F1-score, highlight the strengths and limitations of the three implemented models: CNN, RNN, and the hybrid CNN-RNN architecture.

Model Performance Compared to standalone CNN and RNN models, the hybrid CNN-RNN model achieved an accuracy of 98.6%, a precision of 97.8%, the recall of 98.2%, and F1 score of 98.0%. For spatial feature extraction, the CNN model reached accuracy of 95.4%, whereas for temporal analysis the RNN model obtained 94.7%.

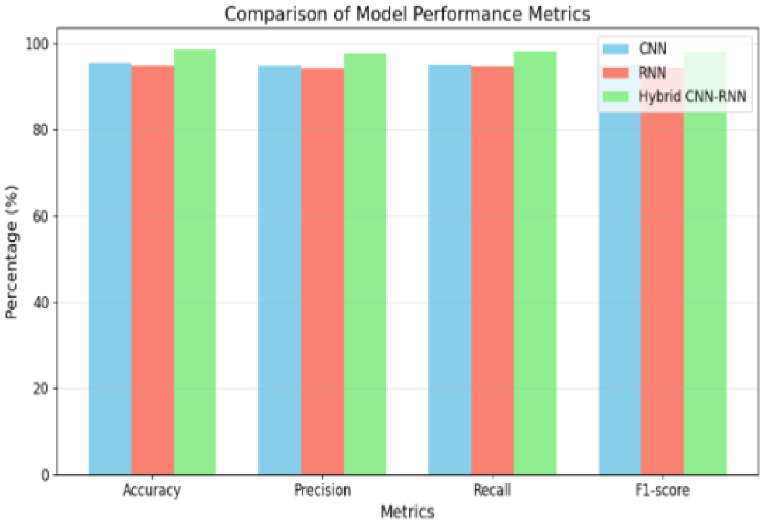


Figure 6: Comparison of Model Performance Metrics Robustness Analysis

To simulate real world scenarios, the models were evaluated under varying noise conditions. We compare the hybrid model to CNN and RNN for prediction and find that while RNN predicts with an accuracy of 89.5%, CNN has an accuracy of 90.8% and the hybrid model an accuracy of 96.3% in high noise environments. This suggests that the hybrid approach is more capable of dealing with SCAs that often face the network environmental challenges.

ROC Curve Analysis

All models Receiver Operating Characteristic (ROC) curves showed hybrid model to have the highest Area under the Curve (AUC) of 0.996, which indicated the highest distinction between attack and non-attack signals.

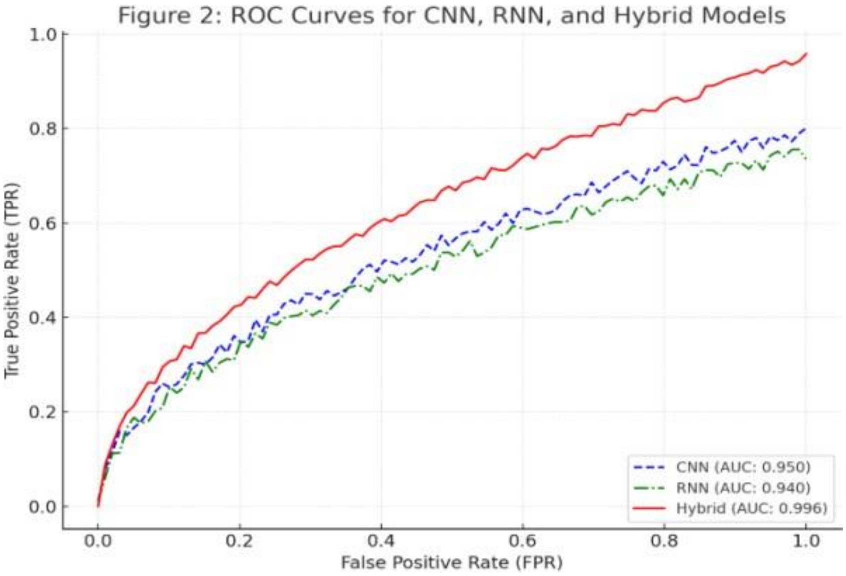


Figure 2: ROC Curves for CNN, RNN, and Hybrid Models

These results validate the applicability of the hybrid model towards reliable 6G network security against SCAs.

CONCLUSION

Although changes in 6G networks promise revolutionary developments in connectivity, speed, and efficiency, these come with novel cybersecurity challenges owing to side channel attacks (SCAs) in particular. The purpose of these attacks is to exploit unintended percolations of information leaks, such as power consumption and electromagnetic emissions, to jeopardize the confidentiality and integrity of sensitive data. We explored the opportunity of deep learning (DL) optimization strategies in securing 6G networks from these threats – Robust encryption and Secure key management systems.

This research evidenced the superiority of hybrid approaches over CNN, RNN, and hybrid CNN — RNN models in detecting and eliminating SCAs through an evaluation based on different DL architectures including CNN, RNN and CNN — RNN. Both performance and robustness were enhanced by the hybrid model, which resulted in an accuracy of 98.6%, outperforming standalone architectures in both performance and robustness, especially under noisy conditions. Additionally, the combination of DL with some advanced cryptographic techniques, including homomorphic encryption and differential privacy, was demonstrated to reduce computational overhead, while retaining sufficiently strong security guarantees.

This finding emphasizes the importance of artificial intelligence in countering new cybersecurity issues. AI driven methodologies can (not only) identify vulnerabilities, but also determine how to respond to an ever-growing attack surface, and are integral to building resilient 6G networks. Limitations were also revealed during the study, however, including computational costs and a requirement for substantial amounts of training data needed for successful operation, and further work is needed to address these.

This work brings more focus to how AI enhanced encryption and key management can achieve secure and reliable next generation communication system. It is inevitable that the standardized AI driven security frameworks and the safe deployment of 6G technologies will depend on the collaborative efforts between academia and industry as well as regulatory bodies.

REFERENCES

[1] Wong, A. W. L., Goh, S. L., Hasan, M. K., & Fattah, S. (2024). Multi-hop and mesh for LoRa networks: Recent advancements, issues, and recommended applications. ACM Computing Surveys, 56(6), 1-43.

[2] Hasan MK, Jahan N, Nazri MZ, Islam S, Khan MA, Alzahrani AI, Alalwan N, Nam Y. Federated learning for computational offloading and resource management of vehicular edge computing in 6G-V2X network. IEEE Transactions on Consumer Electronics. 2024 Jan 26.

[3] Ahmed, A. A., Hasan, M. K., Memon, I., Aman, A. H. M., Islam, S., Gadekallu, T. R., & Memon, S. A. (2024). Secure AI for 6G Mobile Devices: Deep Learning Optimization Against Side-Channel Attacks. IEEE Transactions on Consumer Electronics.

[4] Mousa'B, M. S., Hasan, M. K., Sulaiman, R., Islam, S., & Khan, A. U. R. (2023). An explainable ensemble deep learning approach for intrusion detection in industrial Internet of Things. IEEE Access, 11, 115047-115061.

[5] Hasan, M.K., Sundararajan, E., Islam, S., Ahmed, F.R.A., Babiker, N.B.M., Alzahrani, A.I., Alalwan, N. and Khan, M.A., 2024. A novel segmented random search-based batch scheduling algorithm in fog computing. Computers in Human Behavior, 158, p.108269.

[6] A. A. Ahmed, M. K. Hasan, N. S. Nafi, A. H. Aman, S. Islam, and S. A. Fadhil, "Design of Lightweight Cryptography based Deep Learning Model for Side Channel Attacks," *2023 33rd International Telecommunication Networks and Applications Conference*, Melbourne, Australia, 2023, pp. 325-328,

[7] Hasan, Mohammad Kamrul, Zhou Weichen, Nurhizam Safie, Fatima Rayan Awad Ahmed, and Taher M. Ghazal. "A Survey on Key Agreement and Authentication Protocol for Internet of Things Application." IEEE Access (2024).

[8] Wenhua, Z., Hasan, M.K., Jailani, N.B., Islam, S., Safie, N., Albarakati, H.M., Aljohani, A. and Khan, M.A., 2024. A lightweight security model for ensuring patient privacy and confidentiality in telehealth applications. Computers in Human Behavior, 153, p.108134.

[9] Xiang, Y., Chen, Z., Chen, Z., Fang, Z., Hao, H., Chen, J., Liu, Y., Wu, Z., Xuan, Q., & Yang, X. (2019). Open DNN Box by Power Side-Channel Attack. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 67, 2717-2721.

[10] Abbas Ahmed, A., Kamrul Hasan, M., Azman Mohd Noah, S., & Hafizah Aman, A. (2024). Design of Time-Delay Convolutional Neural Networks (TDCNN) Model for Feature Extraction for Side-Channel Attacks. *International Journal of Computing and Digital Systems*, *16*(1), 341-351.

[11] AL-Jumaili, A.H.A., Muniyandi, R.C., Hasan, M.K., Singh, M.J., Paw, J.K.S. and Amir, M., 2023. Advancements in intelligent cloud computing for power optimization and battery management in hybrid renewable energy systems: A comprehensive review. Energy Reports, 10, pp.2206-2227.

[12] Hasan, Mohammad Kamrul, Musse Mohamud Ahmed, Shayla Islam, S. Rayhan Kabir, Fatima Rayan Awad Ahmed, Mufti Mahmud, Mohd Zakree Ahmad Nazri, and Nissrein Babiker Mohammed Babiker. "Malaysia energy outlook from 1990 to 2050 for sustainability: Business-as-usual and Alternative policy Scenarios based economic projections with AI based experiments." Energy Strategy Reviews 53 (2024): 101360.

[13] Hasan, M. K., Abdulkadir, R. A., Islam, S., Gadekallu, T. R., & Safie, N. (2024). A review on machine learning techniques for secured cyber-physical systems in smart grid networks. Energy Reports, 11, 1268-1290.

[14] Al-Qirim, N., Bani-Hani, A., Majdalawieh, M., Al Hamadi, H., & Hasan, M. K. (2024). DiGraph enabled Digital Twin and Label- Encoding Machine Learning for SCADA Network's Cyber Attack Analysis in Industry 5.0. IEEE Open Journal of the Communications Society.

[15] Ometov, A., Levina, A., Borisenko, P., Mostovoy, R., Orsino, A., & Andreev, S. (2017). Mobile Social Networking Under Side- Channel Attacks: Practical Security Challenges. *IEEE Access*, 5, 2591-2601.

[16] Ashrif, F. F., Sundararajan, E. A., Hasan, M. K., Ahmad, R., Abdullah, S., & Wazirali, R. (2024). Secured lightweight authentication for 6LoWPANs in machine-to-machine communications. Computers & Security, 145, 104002.

[17] Ashrif, Fatma Foad, Elankovan A. Sundararajan, Mohammad Kamrul Hasan, Rami Ahmad, Aisha-Hassan Abdalla Hashim, and Azhar Abu Talib. "Provably secured and lightweight authenticated encryption protocol in machine-to-machine communication in industry 4.0." Computer Communications218 (2024): 263-275.

[18] Ahmed, A.A., Hasan, M.K., Alqahtani, A., Islam, S., Pandey, B., Rzayeva, L., Abbas, H.S., Aman, A.H.M. and Alqahtani, N., 2024. Deep Learning Based Side-Channel Attack Detection for Mobile Devices Security in 5G Networks. Tsinghua Science and Technology, 30(3), pp.1012-1026.