ML-based Real-Time URL Inspection with Hardware Acceleration for Enhanced Web Security

26th International Symposium on Quality Electronic Design (ISQED'25)
San Francisco, California, USA

Majid Nezarat, Erfan Khedersolh, Hadi Shariar Shahhoseini and Amin Rezaei

isQED Symposium 2025

Speaker Bio

Dr. Amin Rezaei is an Assistant Professor in the Department of Computer Engineering and Computer Science at California State University, Long Beach. He obtained his Ph.D. in Computer Engineering from Northwestern University. He has a decade of experience in hardware security, computer architecture, and machine learning, with more than 50 peer-reviewed scientific articles at flagship venues such as DAC, ICCAD, DATE, and ASP-DAC. He is a senior member of IEEE and a lifetime member of ACM and AAAI and has served on the technical program committees of many major conferences in his area.

Agenda

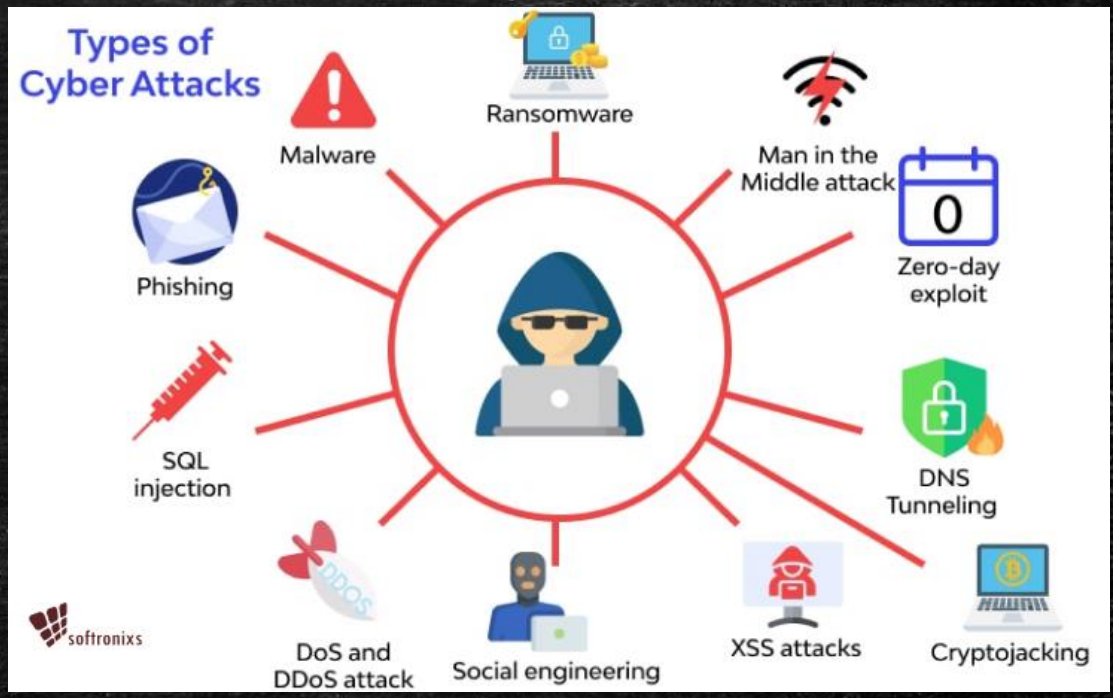
1. Abstract
2. Introduction
3. Related Works
4. Proposed Method
5. Experimental Results
6. Conclusion

Enhancing Web Browsing Security on IoT and Edge Devices

- **Challenge**
  - IoT and Edge devices, due to their resource constraints, lack the capability to implement computationally intensive security mechanisms, making them vulnerable to cyber threats such as phishing and malware.
- **Proposed Solution**
  - A machine learning-based approach for real-time URL inspection to identify and classify malicious websites.
- **Key Features**
  - Categorization of websites into benign, phishing, malware, defacement and spam.
  - Development of a lightweight neural network optimized for resource-constrained hardware.
  - Implementation as either a browser extension or a hardware security module.

Cyber Threats and the Need for Web Security

- **Internet's User Growth & Security Challenges**
  - Internet technology has revolutionized banking, education, and e-commerce.
  - However, cybercriminals exploit vulnerabilities through phishing, malware, and website defacement attacks.



https://softronixs.com/

Cyber Threats and the Need for Web Security

- **Why Malicious Websites Are a Major Threat**
  - Many cyberattacks rely on fake or compromised websites to steal user data.
  - Early detection and blocking of malicious URLs can significantly enhance cybersecurity.

https://industrialcyber.co/

Proposed Solution – Real-Time URL Classification

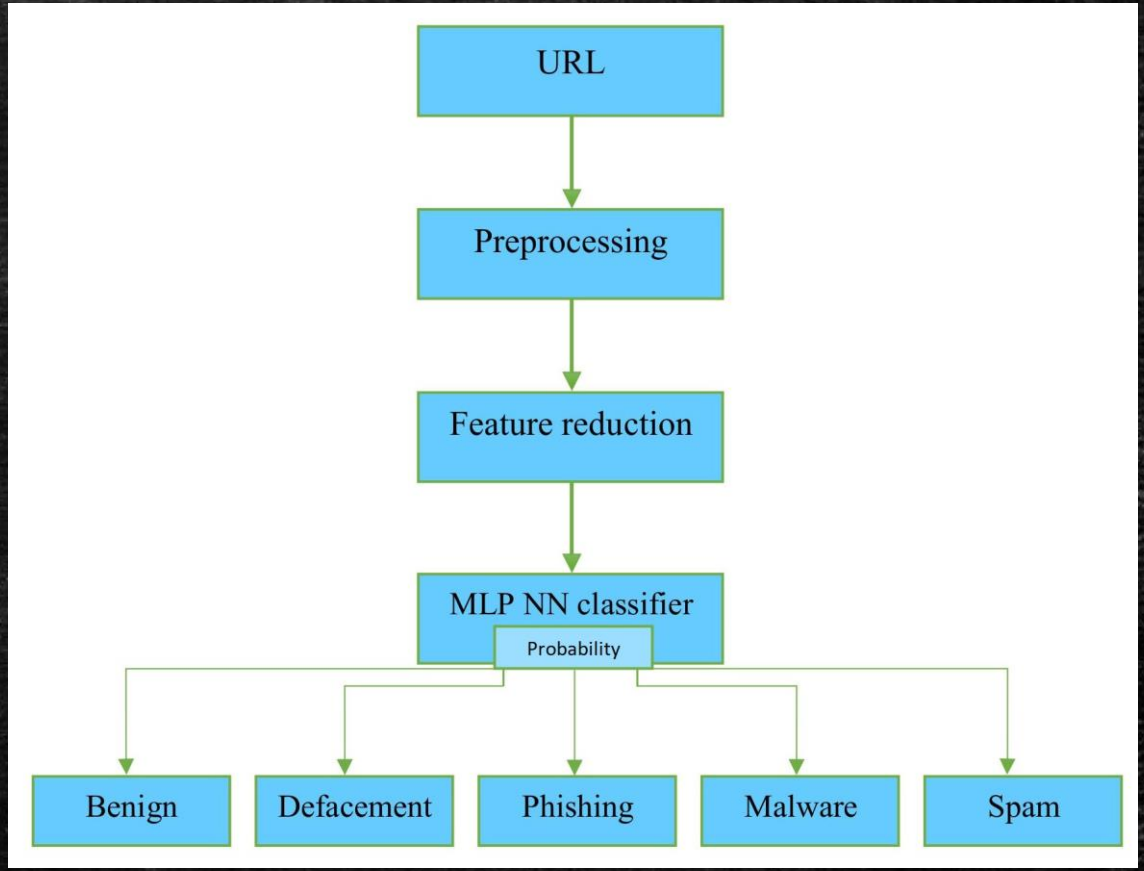
- **Machine Learning for Web Security**
  - Extracting key features from URLs to classify websites as safe or malicious.
  - Training a lightweight neural network (MLPNN) to ensure accurate, fast detection.
- **Hardware-Optimized Implementation**
  - Low power consumption and minimal resource usage, making it ideal for IoT devices.
- **Key Benefits**
  - High accuracy in detecting cyber threats.
  - Seamless performance without slowing down web browsing.
  - Practical deployment for enhanced IoT and Edge security.

Review of Existing URL Detection

- **Black & White List**
  - URL detection methods based on black & white lists consist of two lists of allowed and unallowed URLs.
  - Vulnerability to zero-day attacks and unfairly group reports are weaknesses of list-based systems.
- **Machine Learning**
  - Machine learning is the most popular method for identifying and predicting malicious URLs.
  - The primary challenge lies in the real-time implementation of machine learning algorithms on edge devices.

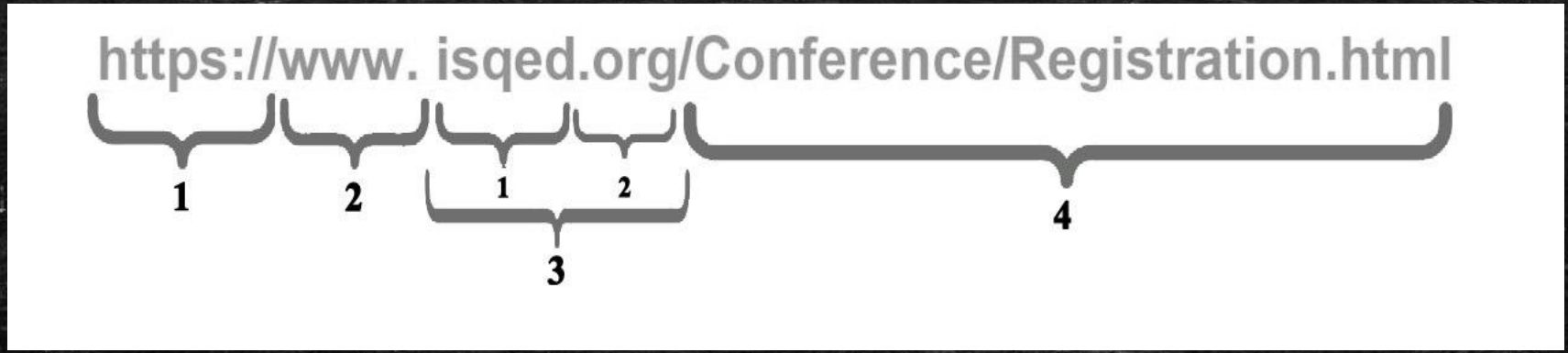
MERCEDES

- **Propose MERCEDES: An ML-based rEal-time URL inspeCtion for EnhanceD wEb Security**



URL Features and Dataset

- **URL Features**
  - URLs contain a wealth of hidden information that can be classified by machine learning algorithms based on these features.



- **Dataset**
  - dataset that has been used was collected by Canadian Institute of Cyber Security (CIC) and contains five different classes.

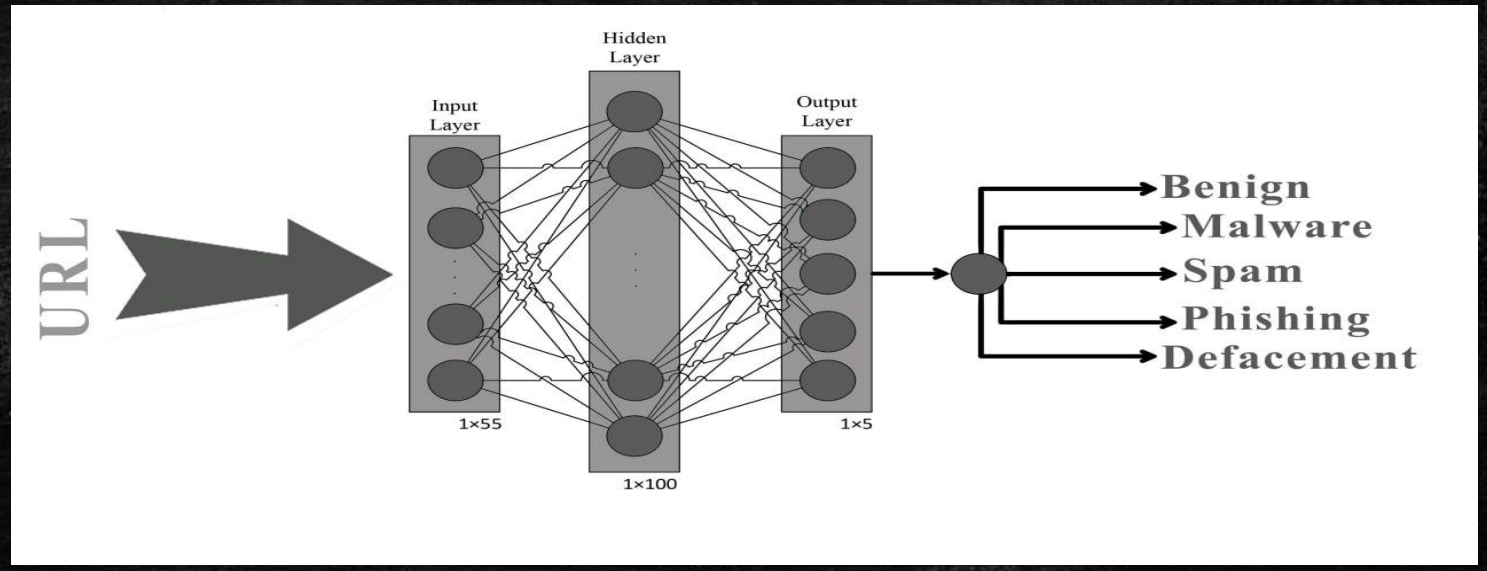
Feature Reduction and Preprocessing

- **Preprocessing**
  - After converting all features to numbers, all numbers (features) are mapped between 0 and 1.
- **Feature Reduction**
  - PCA has been used to reduce the feature dimensions. PCA has increased the accuracy and also reduced the storage space of the model.

Parameter	Without PCA	With PCA
Features	79	55
Total Parameters	8505	6105
Occupied memory (KB)	33.22	23.85
Accuracy (after 25 epochs) (%)	94.75	95.13
Accuracy (after 50 epochs) (%)	96.31	96.57
Accuracy (after 100 epochs) (%)	96.82	96.98
Accuracy (after 200 epochs) (%)	96.82	97.68

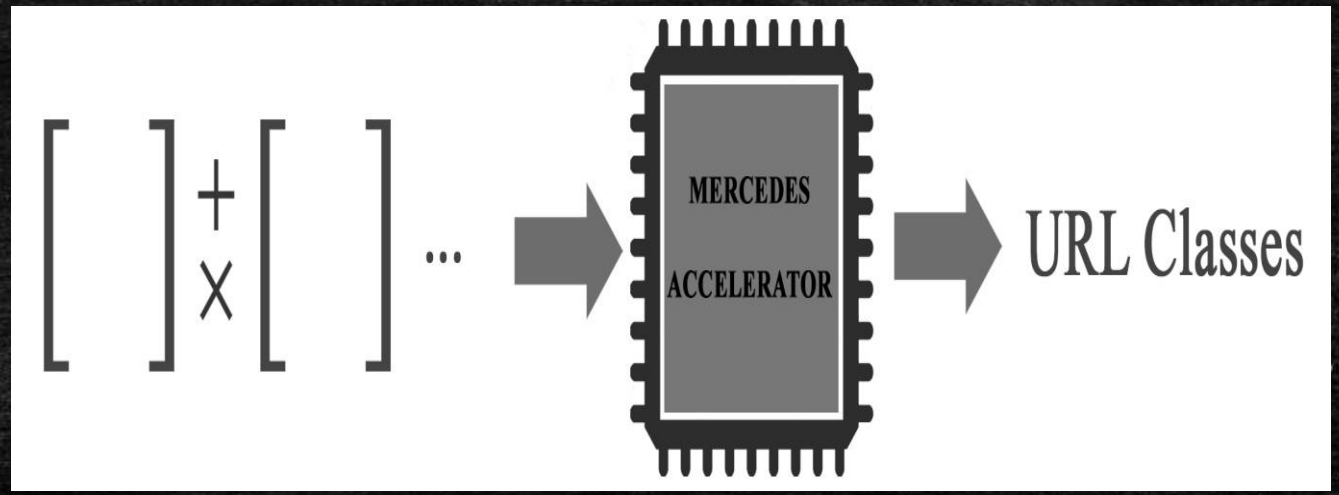
MLP NN Classifier

- **MLP NN Design**
  - Due to the importance of reducing computational overhead, the proposed neural network has only one hidden layer.
- **Computational Model Extraction**
  - After training the neural network, a computational model of matrix addition and multiplication is extracted from the model so that it can be implemented on hardware with the best performance.



Hardware Implementation

- **Computable Neural Network**
  - The MLP NN was transformed into matrix multiplication, addition and determinant.
- **Hardware Design Using FPGA**
  - The design is carried out with a focus on optimizing power consumption, processing speed, and resource utilization.



Classifier Results

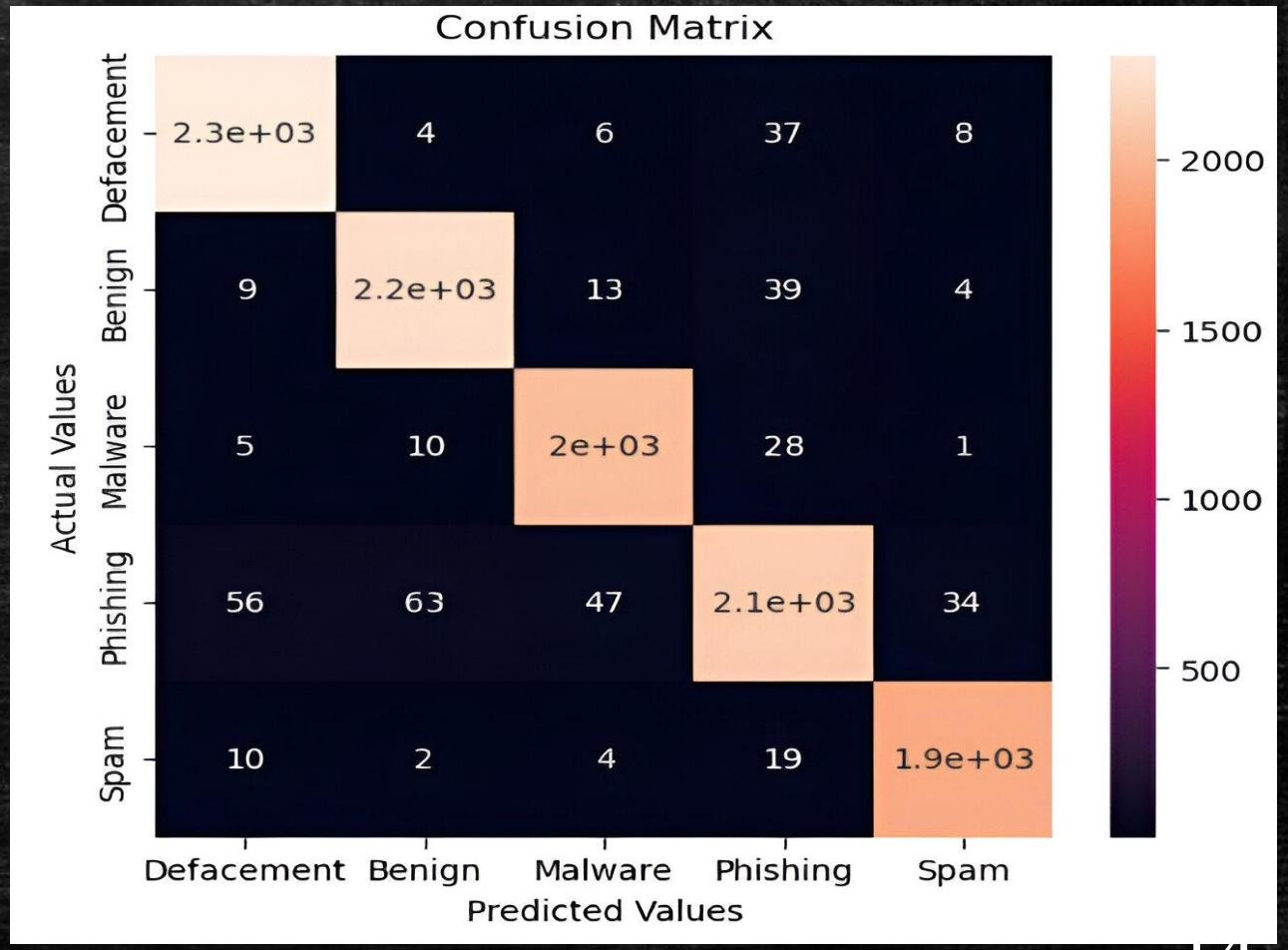
- **Accuracy**

	Accuracy	Recall	Precision	F1 Score
MERCEDES	97/68%	97/08 %	98/17 %	97/62 %
HMLM [1]	98/12 %	96/33 %	97/31 %	95/89 %
BLSTM [2]	95/47 %	95/37 %	95/6 %	95/67 %
TMMUC [3]	98/55 %	98/57 %	98/55 %	98/56 %

- **Total Parameters**

Model	Parameter
Hidden Layer (Type, Dimension)	Dense, [1,100]
Output Layer (Type, Dimension)	Dense 1, [1,5]
Trainable Parameters (Number, Size)	6105, 23.85 KB
Not Trainable Parameters (Number, Size)	0, 0 KB

- **Confusion Matrix**



Hardware Results

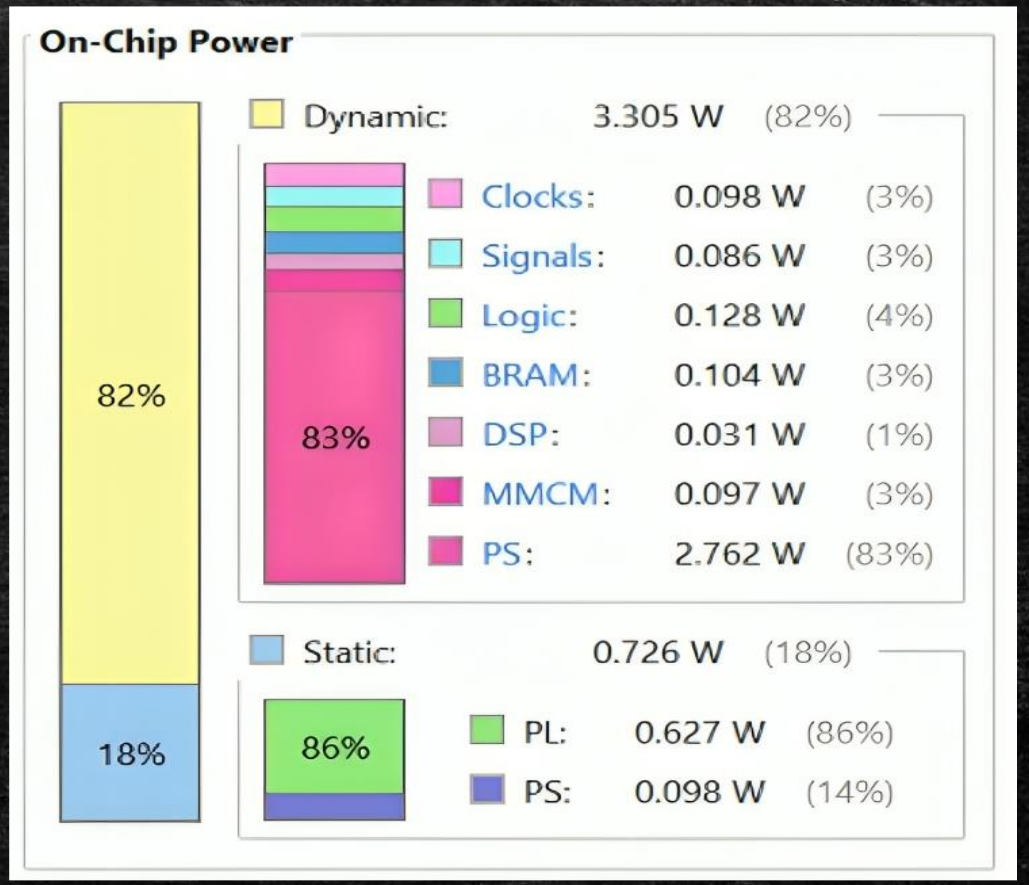
- **Timing Parameters**

	Timing
CLOCK Target	4.00 ns
CLOCK Estimated	3.454 ns
CLOCK Uncertainly	0.50 ns
Latency (Cycles)	63244 cycles
Latency (Absolute)	253,000 ns

- **Resource Utilization**

RESOURCE	UTILIZATION
CLB LUTs	0.44%
CLB Registers	0.17%
CARRY8	0.22%
CLB	0.74%
LUT as Logic	0.42%
LUT as Memory	0.03%
Block RAM	3.50%
DSPs	0.63%
Others	0.0%

- **Power Consumption**



Conclusion and Future Work

- **Conclusion**
  - In this paper, the proposed lightweight neural network can have high accuracy and at the same time have very low execution time.
  - The proposed approach can be embedded inside edge devices and protect them from cyberattacks.
- **Future Work**
  - Further research is focused on identifying malware that resides in memory and will show its effects during processing.

References used for Comparison

- [1] A. Karim, M. Shahroz, K. Mustofa, S. B. Belhaouari, and S. R. K. Joga, “Phishing detection system through hybrid machine learning based on URL,” In IEEE Access, vol. 11, pp. 36805-36822, 2023.
- [2] S. Wang, S. Khan, C. Xu, S. Nazir, and A. Hafeez, “Deep learning-based efficient model development for phishing detection using random forest and BLSTM classifiers,” In Complexity, vol. 2020, pp. 1–7, 2020.
- [3] N. Q. Do, A. Selamat, K. C. Lim, O. Krejcar, and N. A. Md. Ghani, “Transformer-based model for malicious URL classification,” In IEEE International Conference on Computing (ICOCO), pp. 323-327, 2023.

THANK YOU!