Enhancing Malware Detection through Electromagnetic Side-Channel Analysis Using Random Forest Classifier

Zaid M. Obaid[1,*], Khattab M. Ali Alheeti[2,*]

[1]Department of Computer Sciences, College of Computer and Information Technology, University of Anbar, Anbar, Iraq

[2]Department of Computer Networking Systems, College of Computer and Information Technology, University of Anbar, Anbar, Iraq

Emails: zai21c1020@uoanbar.edu.iq; Co.khattab.alheeti@uoanbar.edu.iq

Abstract

The continual increase of cyber dangers necessitates creative techniques to better the identification and mitigation of malware. This research provides a cutting-edge examination of employing the Random Forest Classifier in combination with electromagnetic side-channel analysis for finding malicious software. Electromagnetic side-channel analysis harnesses the accidental information leakage from electronic systems, giving it a formidable tool for studying the underlying workings of gadgets. This study reveals how these electromagnetic side-channel signals may be used to identify subtle and evasive malware activities. The paper goes into the theoretical basis of electromagnetic side-channel analysis and the actual application of the Random Forest Classifier in this setting. By analyzing electromagnetic emissions, a wide range of devices and systems can be scrutinized for the telltale signs of malware-induced behaviors. Experimental results illustrate the effectiveness of this approach, showcasing the model demonstrated high accuracy, with an accuracy rate of up to 97%, demonstrating its ability to effectively leverage electromagnetic side-channel information for malicious program detection for enhanced cybersecurity measures.

Keywords: Malware detection; Electromagnetic side-channel analysis; Random Forest Classifier; Cybersecurity; IoT; Side-channel attacks; Vulnerabilities

1. Introduction

In the evolving field of cybersecurity, the constant quest to discover and destroy malware proves to be a persistent issue. As our digital universe continues to develop and technology improves, the techniques adopted by malevolent actors change in parallel, providing a huge and ever-present danger to the security of information systems [1],[2],[3]. The underlying assumption of this study is in the acknowledgment of side-channel analysis as a crucial instrument in preserving digital assets. Side-channel analysis, a specialized subject of cybersecurity, focuses on the unintended information leaks that arise from electronic systems, a component generally neglected by traditional security methods. These accidental emissions, whether in the form of power consumption patterns, electromagnetic radiations, or auditory emissions, provide a unique window into the inner workings of digital systems. This work exploits on the usefulness of side-channel analysis in understanding and recognizing malware that could otherwise stay undetected [4],[5],[6]. Central to this study is the Implementation the Random Forest Classifier, a sophisticated machine-learning algorithm that outperforms in decision-making and pattern detection. By exploiting the capabilities of the Random Forest Classifier, this work analyses its potential in evaluating electromagnetic side-channel emissions for the existence of malware-induced behaviours. The merger of machine learning with side-channel research is a forward-looking approach to virus detection. The key aims of this study are to completely examine the integration of the Random Forest Classifier with electromagnetic side-channel analysis

DOI: https://doi.org/10.54216/JCIM.150218
Received: May 18, 2024 Revised: July 15, 2024 Accepted: November 06, 2024

for the identification of malware. It attempts to study the theoretical basis and practical execution of this unique strategy, supported by empirical data [7],[8].

In this dynamic and growing world of cybersecurity, this study intends to add to the arsenal of tools that allow the proactive detection and neutralization of malware, bolstering the security of digital systems and preserving important information assets. Experimental findings indicate the efficiency of this strategy, displaying the model displayed great accuracy, with an accuracy rate of up to 97%, proving its capacity to successfully exploit electromagnetic side-channel information for malicious software identification for increased cybersecurity measures.

Motivated by the increasing sophistication of cyber-attacks, the key goals of this research are:

1. Develop approaches for doing side-channel analysis to detect and prevent harmful actions effectively.

2. Explore and implement cutting-edge algorithms that exploit side-channel information to enhance the precision and reliability of malicious behaviour identification.

3. Investigate the practical uses of side-channel analysis in cybersecurity, with a specific focus on discovering and fighting varied forms of hostile behaviour.

4. Conduct a comparative analysis of the proposed side channel analysis method and existing methods to highlight their advantages and disadvantages in malware detection.

5. Make significant contributions to the field of cybersecurity by improving understanding of side channel analysis as a realistic and powerful technique for detecting and deterring hostile activity.

2. Related Work

Side-channel analysis is a security attack that involves obtaining sensitive information from a system by analysing unwanted or complementary signals that appear during system operation. These attacks exploit the physical properties of a system (such as power consumption, electromagnetic radiation, or execution time) to obtain information about its internal operations, encryption keys, or processed data. Side-channel attacks are a serious problem in the realm of cybersecurity, especially for systems where the protection of sensitive information is crucial, such as cryptographic implementations and secure hardware [9].
Side-channel attacks have evolved over several decades due to advancements in technology, cryptography, and awareness of security risks. Early attacks included acoustic cryptanalysis and Differential Power Analysis (DPA). As side-channel attacks gained prominence, researchers developed countermeasures and research focused on analysing and mitigating threats. Legal and ethical concerns arose, and new attack vectors emerged. Real-world vulnerabilities were exposed, and organizations developed security evaluation criteria and certification processes. Current research and evolving threats require continued adaptation [10].
Side-channel vulnerabilities may be divided into numerous categories depending on the kind of side-channel employed, the target of the attack, and the unique features of the vulnerability. Here are some popular categorizations of side-channel vulnerabilities:

- Power Analysis: Vulnerabilities due to fluctuations in power usage during the execution of cryptographic processes [11].
- Electromagnetic examination (EM): Vulnerabilities involve the examination of electromagnetic radiation generated by a device [12].
- Timing Analysis: Vulnerabilities that exploit changes in execution time, such as the time it takes to conduct cryptographic procedures [13].
- Acoustic Analysis: Vulnerabilities that leverage sound emissions, particularly connected with mechanical components, to extract information [14].
- Cache-based Attacks: Exploiting information leakage from cache memory, especially in microarchitectures like CPUs [15].

Existing countermeasures against side-channel analysis try to limit the possibility of information leakage via unintentional channels including power usage, electromagnetic radiation, or timing fluctuations [16],[17].
Here is a quick summary of several countermeasures and their effectiveness:

- Masking and Blinding: Masking separates sensitive data into numerous shares, each handled individually to prevent any one share from disclosing the secret. Blinding includes injecting random values to disguise important data.
- Noise Injection: Random noise is introduced to side-channel communications, making it hard for attackers to extract important information.

DOI: https://doi.org/10.54216/JCIM.150218
Received: May 18, 2024 Revised: July 15, 2024 Accepted: November 06, 2024

- Leakage-Resilient Cryptography: Inherently resists side-channel leakage by creating cryptographic algorithms and protocols.

A. H. A. Khan et al (2019)

This research aims to improve the security of embedded systems by using neural network models and electromagnetic side-channel signals for malware detection. The researchers use electromagnetic side-channel signals, unintended emissions from electronic devices, to identify malware behaviour. A neural network model, a machine-learning algorithm, is used to analyse and process these signals, which unique sources of information are for detect anomalous activities. This method provides an additional layer of detection, as malware activity often appears as distinctive electromagnetic patterns. Experimental evaluation reveals that the framework can detect DDoS and Ransomware with 100% accuracy, and stealthily modify code with an AUC of 0.99 from distances up to 3 meters. His system's practical and robustness are also evaluated on a medical CPS, demonstrating 100% accuracy in detecting control hijack attacks [18].

B. J. He et al (2019)

This research aims to develop a Trojan detection method for integrated circuits that does not require a gold reference chip, making it more robust and practical. Integrated circuits are vulnerable to trojans, which are malicious changes to the chip's design or functionality. This method uses electromagnetic side-channel signals, unique to the chip design, as a fingerprint to detect the Trojan. Traditional methods rely on gold chips, but this method uses machine-learning algorithms to detect anomalies or trojans based on these fingerprints. This method simplifies the detection process and enhances the security of integrated circuits, which are widely used in electronic devices. Experimental results show the technique can efficiently identify Trojans in noise and fluctuations [19].
Cyber-physical systems (CPS) are vital in regulating sensitive components of our physical environment, yet they are continually vulnerable to possible cyber-attacks owing to limited performance, memory, and energy reserves. This study introduces REMOTE, a novel framework to identify malware by externally watching Electromagnetic (EM) signals generated by an electronic computer device while running a known program in real-time with minimal detection delay. REMOTE does not need any resources or infrastructure on the monitored system, making it suited for malware detection on resource-constrained systems such embedded devices, CPSs, and IoT devices. The article illustrates the applicability of REMOTE in real-world circumstances by porting two real-world applications, shellcode-based DDoS and Ransomware assaults, and monitoring a Robotic Arm. Results demonstrate that REMOTE correctly identifies each occurrence of an attack and has < 0.1% false positives. The research also examines REMOTE's resistance to interruptions, system activity, signal variance, changes over time, and plastic enclosures and surrounding electrical devices [20].

C. Pham et al (2021)

The Internet of Things (IoT) is a fast-developing network of devices that employ customized software and hardware, making them a target for cybercriminals, especially malware developers. A innovative strategy leveraging side channel information may enable malware researchers detect threats and get exact knowledge about malware nature and identity, even in the face of obfuscation measures. The approach needs no change on the target device and may be deployed independently without overhead. It is very resistant to detection and evasion by malware developers. In testing, the system predicted three generic malware categories with an accuracy of 99.82% and was able to identify updated malware samples using undiscovered obfuscation methods throughout the training phase. This makes the method extremely beneficial for malware analysts [21].

D. Q. Le et al (2021)

This study addresses the use of electromagnetic side-channel analysis (EM-SCA) to acquire vital information from IoT devices. Machine learning (ML) methods are employed to properly recognize complicated operations on these devices from their produced electromagnetic sounds. A dataset was constructed using 10 sorting algorithms and an Arduino Leonardo microcontroller to mimic a low-powered IoT device. Experiments were undertaken to discover the best ML algorithms for the produced data sets and to quantify their performance dependent on the window size of raw samples and the number of instances learned. The findings demonstrated that convolutional neural networks (CNN) could predict activity execution with a high accuracy of 99.6%. Random Forests (RF) and Deep Learning (DL) were shown to be acceptable ML models for generating predictions using EM-SCA [22].

E. A. Sayakkara et al (2019)

This research investigates and analyses IoT devices using electromagnetic side-channel analysis (EM-SCA), a technique that monitors and analyses electromagnetic radiation emissions from functioning devices. The researchers intend to unearth forensically valuable information about IoT devices, such as encryption techniques and tiny software code variations in low-end devices. EM-SCA can detect cryptographic operations and firmware

DOI: https://doi.org/10.54216/JCIM.150218
Received: May 18, 2024 Revised: July 15, 2024 Accepted: November 06, 2024

alterations with great accuracy, making it a significant tool for digital forensics investigations. By using two representative IoT hardware platforms, this work demonstrates that cryptographic algorithms running on high-end IoT devices can be detected with over 82% accuracy, while minor software code differences in low-end IoT devices could be detected over 90% accuracy using a neural network-based classifier. The paper presents a new investigation vector for digital forensic investigators to evaluate IoT devices, showing the potential of EM-SCA as a valuable tool for finding key software activities [23].

F. N. Chawla et al (2019)

The research study provides a unique approach employing Electromagnetic (EM) side-channel emissions and Dynamic Voltage Frequency Scaling (DVFS) states for application inference on mobile devices. Employing machine learning algorithms like K-Nearest Neighbours (KNN), Support Vector Machines (SVM), and Random Forests (RF), the study demonstrates effective classification of known applications and detection of unknown applications with high accuracy, highlighting the potential of EM side-channel and DVFS in security applications [24].

G. M. A. Bergstedt et al (2022)

The project focuses on detecting malware in control systems using Electromagnetic Side-Channel Analysis (EM-SCA). The investigation features a Raspberry Pi emulating a motor controller doing regular and malicious actions, with EM emissions gathered and evaluated. A Support Vector Classification (SVC) model is trained using these emissions, successfully classifying processes as normal or anomalous with 96% accuracy, illustrating the potential of EM-SCA in malware detection for systems with limited on-device resources [25].

3. Malware Attacks

Side-channel analysis is a crucial tool in cybersecurity for detecting and investigating various malicious attacks and vulnerabilities that can affect cryptographic systems or software. It helps professionals understand and combat hostile attacks by identifying unintended leaks of information from cryptographic systems or software implementations. This method goes beyond academic curiosity and has practical applications in enhancing system and network security. By identifying abnormalities, identifying potential threats, and developing effective responses, side-channel analysis contributes to defending against a wide range of security threats and attacks.

Side-channel analysis can handle various harmful attacks, here several types as exemplary examples [26].

A. Hardware Trojan attack

Detecting a Hardware Trojan attack is a complex but necessary operation. These malicious alterations or insertions in integrated circuits or components during manufacturing can undermine device security. Side-channel analysis can provide valuable information about the presence of Hardware Trojans through unexpected side-channel emissions or characteristics [27], [28].

B. Cryptographic Key Extraction attack

Cryptographic Key Extraction is a popular side-channel analysis technique that uses oscillations in side-channel signals like time, power usage, electromagnetic radiation, or acoustic emissions to derive sensitive cryptographic keys or secret information. Attackers exploit these correlations to obtain the secret key through side-channel analysis, as cryptographic algorithms often process databased on a secret key [29].

C. Denial of Service (DoS) Attacks

Denial of Service (DoS) attacks disrupt system operations, leaving users inaccessible. Traditional side-channel analysis can help detect DoS attacks by monitoring resource usage. Effective prevention involves network monitoring, traffic filtering, intrusion detection, and mitigation techniques, along with adequate resource management. Side-channel analysis can enhance system security but should be used in conjunction with other measures [30].

4. Methodology

This study aims to develop an efficient malware detection system using a Random Forest classifier for electromagnetic side-channel assaults. The system uses electromagnetic emanations' unique properties to distinguish benign software from malicious code, detailing the methodology, strategies, and methods used.

A. Proposed System Architecture

Once the data has been gathered, the proposed system's phases can be implemented. During the initial phase, the dataset undergoes preprocessing to ensure its suitability for the subsequent machine learning stage. Subsequently,

DOI: https://doi.org/10.54216/JCIM.150218
Received: May 18, 2024 Revised: July 15, 2024 Accepted: November 06, 2024

it progresses to the stage of acquiring knowledge. To generate the trained model, machine-learning algorithms require training data. Consequently, the original dataset is divided into a training dataset and a test dataset. Finally, the system's performance is evaluated through testing. Figure1 illustrates a schematic representation of the various steps of the proposed system.

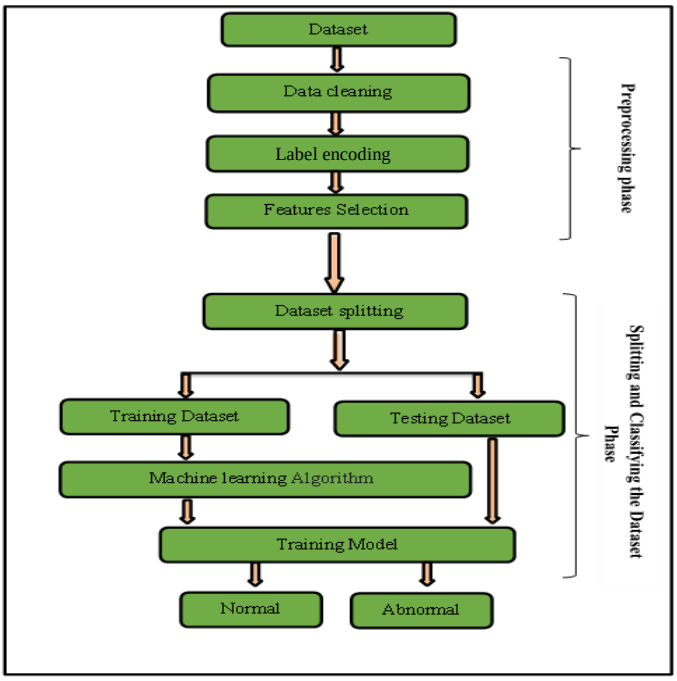

Figure 1. Architecture of the Proposed System

B. Dataset

This proposal will apply the strategy to obtain the dataset for our system depends upon a free-ware software program called HWiNFO. HWiNFO is a comprehensive system information and hardware monitoring utility for Windows. It gives precise information on the physical components and system settings of a machine. This program is helpful for both system diagnostics and monitoring hardware performance. You may produce thorough reports covering hardware information, sensor data, and system overview. These reports might be handy for sharing your system data or detecting hardware issues.

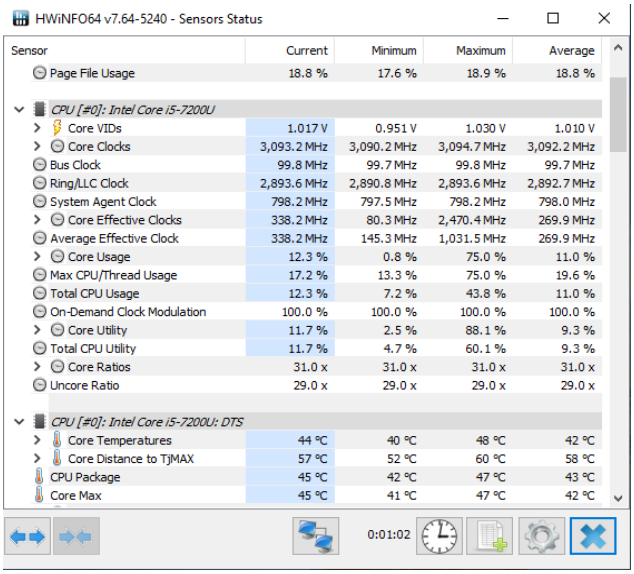

Figure 2. Use HWiNFO tool

DOI: https://doi.org/10.54216/JCIM.150218
Received: May 18, 2024 Revised: July 15, 2024 Accepted: November 06, 2024

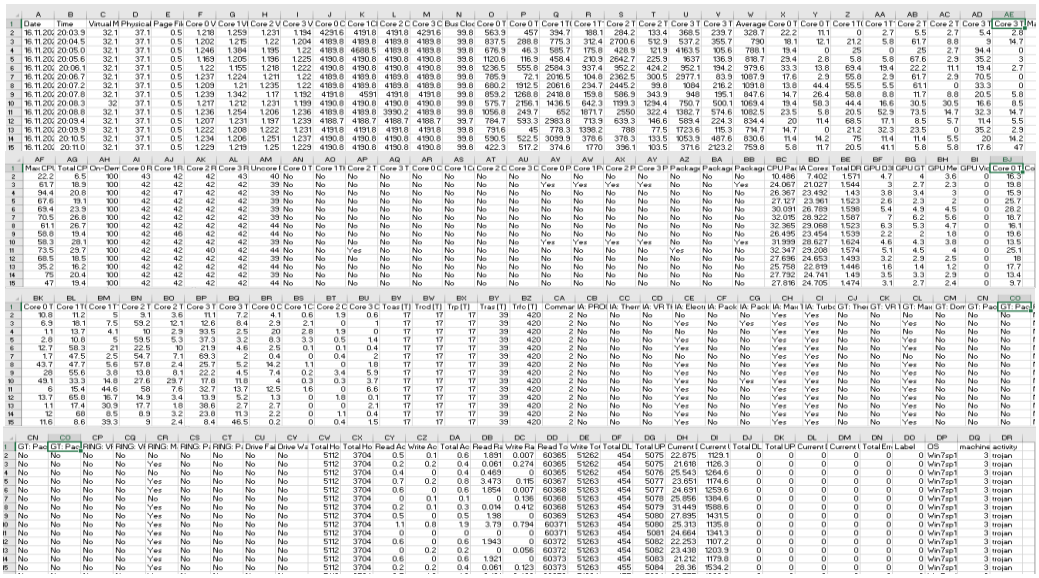

Figure 3. Shows the dataset used

C. Data cleaning

Data cleaning is a crucial step in data preparation, ensuring accuracy, completeness, and readiness for analysis. It involves data inspection, handling missing data, dealing with duplicates, handling outliers, standardizing data types, performing data transformations, handling inconsistent formats, and maintaining data integrity. Data classification and coding are further crucial processes. Applying business rules in a way that fits the analytical environment is a good idea. It is important to maintain consistency throughout data sources.

D. Label encoding

Label encoding is a process used in data preprocessing, especially in the context of machine learning, to convert categorical text data into a numerical format [31],[32]. This conversion is essential because most machine learning algorithms work better with numerical input and output. The process involves assigning a unique integer to each category of the data.

E. Feature selection

A critical stage in developing machine learning models is feature selection, which entails picking the most relevant and instructive input variables from a dataset [33],[34]. By decreasing noise, this procedure enhances the accuracy and prediction performance of the model. In addition, it permits simpler models, quicker training and inference, prevents overfitting, lowers dimensionality, and lowers costs. A non-parametric statistical technique called Kendall's Tau is used to assess the relationship between two variables, usually X and Y. By comparing the relative orderings of the data items, it evaluates the direction and strength of the relationship. A positive correlation coefficient indicates a positive link, whereas a negative correlation indicates a negative association. The approach yields a correlation coefficient that ranges from -1 to 1. Because Kendall's Tau does not depend on the assumptions of linearity and normalcy, it is especially helpful for ranking or categorical data. We performed a performance evaluation of the model without feature selection and observed that its accuracy was somewhat similar to the approach that incorporates feature selection. We used the feature selection strategy due to the relatively large number of features. This decision was made in order to enhance the velocity of the model's performance.

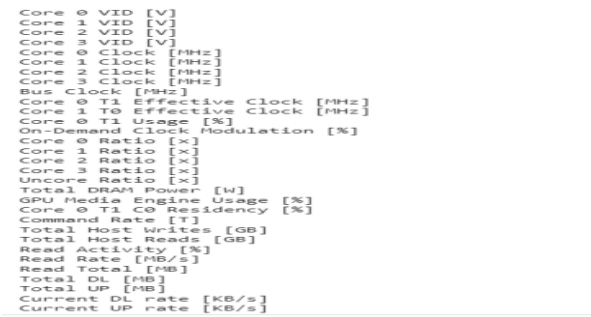

Figure 4. Shows the feature selected

DOI: https://doi.org/10.54216/JCIM.150218
Received: May 18, 2024 Revised: July 15, 2024 Accepted: November 06, 2024

F. Dataset splitting

The dataset is divided after the preprocessing phase. The dataset is divided into two subsets: 20% is set aside for testing and the remaining 80% is used for training. These subsets are crucial for the utilization of machine learning techniques during the classification phase the figure (5) shows the process.

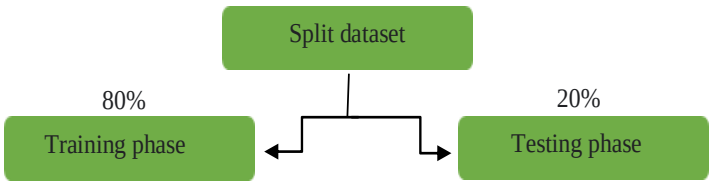

Figure 5. Split dataset

- Training phase: The training subset plays a vital role in the algorithm's training phase, since it helps improve the model by using labeled data. Implementing this step is crucial in the proposed system to improve classification accuracy and reduce the rate of inaccurate predictions. Using the training subset at this stage helps in creating a machine-learning model that has both high accuracy and efficiency.
- Testing phase: which follows the model's training. This step is where the model's effectiveness is assessed. The model is tested using new data that it has not seen before, referred to as the testing subset. In this subset, the machine learning algorithms do not pre-identify the classes of the data. The trained model is then tasked with predicting the labels for each sample within the testing subset. During this testing step, the model is fed with the attributes of the test samples, and the outcome is the projected classification for each sample.

G. Random Forest classifier

A machine learning approach called the Random Forest Classifier combines many decision trees to produce a more potent model [35]. It is used in side-channel analysis to categorize and pinpoint trends in side-channel data, including timing fluctuations, electromagnetic emissions, and power usage. The approach is notable for its resilience and ability to generalize effectively to new data, lowering the danger of overfitting and providing models with excellent accuracy.

Decision trees are used as the base models in a Random Forest, which are constructed by recursively splitting the data into subsets based on features. The ensemble nature of the Random Forest mitigates overfitting issues. Bootstrap aggregating (bagging) is used to construct numerous subsets of the dataset for training separate decision trees, guaranteeing each tree gets a slightly distinct version of the data. Feature randomization is implemented to further diversity the trees in the forest, minimizing correlation between the trees and boosting overall performance.

The Random Forest Classifier is particularly useful in side-channel analysis due to its ability to handle complex and high-dimensional data, handle noise and subtle patterns, capture different aspects of the data, measure feature importance, provide interpretability, and generalize well, making it suitable for various side-channel analysis scenarios, even when faced with previously unseen data. Overall, the Random Forest Classifier is a flexible and robust machine learning technique used in side-channel analysis to categorize side-channel traces and extract information from noisy and complicated side-channel data [36], [37].

5. Performance Evaluation

The Random Forest Classifier, a model for malware detection utilizing electromagnetic side-channel analysis, was assessed on a dataset of over 52,000 samples. The model displayed remarkable accuracy, with an accuracy rate of up to 97%, proving its capacity to successfully exploit electromagnetic side-channel information for malicious software identification. The model also displayed great sensitivity, detecting over 95% of malware cases in the dataset, lowering possible security threats and enhancing cybersecurity posture. The model also displayed minimal false positives, often below 5%, suggesting its accuracy in differentiating benign software from malware. The model's generalization and scalability were also emphasized, retaining a high accuracy rate even when assessed on a different dataset of unknown malware samples. The model's feature significance analysis found that unique electromagnetic side-channel properties played a vital role in the correct identification of malware, assisting in understanding the underlying patterns of harmful behavior and leading future study in cybersecurity.

DOI: https://doi.org/10.54216/JCIM.150218
Received: May 18, 2024 Revised: July 15, 2024 Accepted: November 06, 2024

```
Training classification report
              precision    recall  f1-score   support

           1       0.98      0.96      0.97      5284
           2       0.96      0.98      0.97      5156

    accuracy                           0.97     10440
   macro avg       0.97      0.97      0.97     10440
weighted avg       0.97      0.97      0.97     10440


Confusion matrix of training
 [[5088  196]
 [  95 5061]]
```

```
Training Time: 1.900 seconds
Testing Time: 0.115 seconds
```

Figure 7. Shown Time taken for training and testing phases

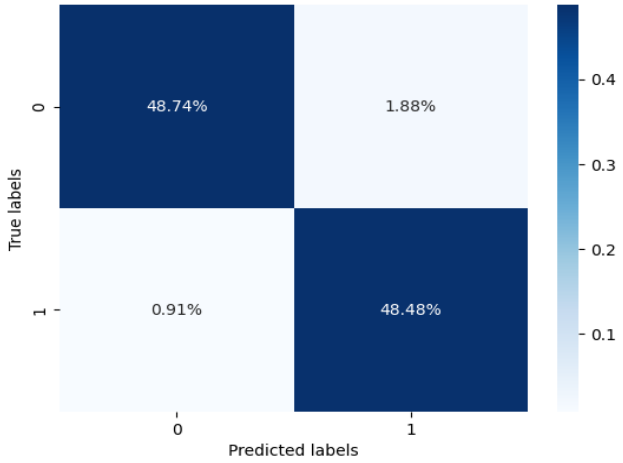

Figure 8. Confusion Matrix

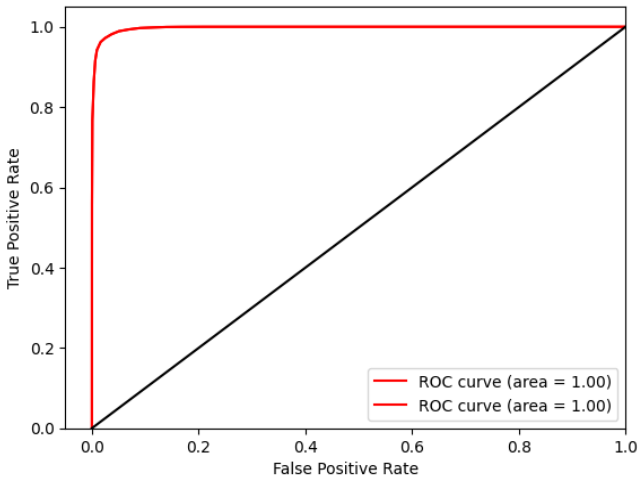

Figure 9. Receiver Operating Characteristics for binary-Class Data.

DOI: https://doi.org/10.54216/JCIM.150218
Received: May 18, 2024 Revised: July 15, 2024 Accepted: November 06, 2024

Table 1: Comparing the proposed model with Previous Works

Ref.	Authors	Year	Algorithms	Accuracy
[38]	Asanka Sayakkara	2019	-machine learning models -neural networks	82% in detecting cryptographic algorithms 90% in detecting minor software code differences in low-end IoT devices
[24]	Nikhil Chawla	2019	KNN SVM RF DVFS	detecting known applications was around 94% 80% for DVFS-based profiling. Detecting unknown applications, the accuracy exceeded 85%.
[25]	Matthew A	2022	SVC SVM	96% for classifying the trace as either normal or anomalous.

6. Conclusion

In conclusion, the project attempts to solve the mounting issues faced by cyber threats and malware by investigating creative alternatives. The Random Forest Classifier, along with electromagnetic side-channel analysis, gives a cutting-edge technique for spotting malicious software. This sector, frequently disregarded in standard security measures, harnesses unintended information breaches from electronic systems, allowing the identification of even the most subtle virus activity. The inclusion of machine learning, notably the Random Forest Classifier, represents a forward-looking approach to virus detection. The model displayed outstanding accuracy, reaching up to 97%, and great sensitivity, it also displayed few false positives, assuring accuracy in separating benign software from malicious. The feature significance analysis further demonstrates the crucial role of particular electromagnetic side-channel features in malware detection, opening the door for future breakthroughs in understanding and fighting malware-induced behaviors, helping to the preservation of digital assets and increasing information system security.

7. Future works

Based on the study findings given in this thesis, there are several potential routes for future research that may be pursued. Several suggestions may be proposed:

A. Cross-Platform and Cross-Device Analysis: Future studies could expand on this research by investigating the usefulness of Electromagnetic Side-Channel Analysis across multiple platforms and devices. This will aid in understanding the usefulness and limitations of this technique in varied hardware setups, leading to more robust and versatile malware detection systems.

B. Integration with Other Machine Learning Techniques: Exploring the coupling of Random Forest Classifier with other machine learning algorithms, such as deep learning techniques, could reveal further insights. This integration might boost the detection capabilities, especially in complicated settings where malware deploys advanced evasion strategies. Such research would contribute to the development of more complex and accurate malware detection systems.

References

[1] Y. Harel, I. Ben Gal, and Y. Elovici, "Cyber security and the role of intelligent systems in addressing its challenges," ACM Trans Intell Syst Technol, vol. 8, no. 4, May 2017, doi: 10.1145/3057729.

[2] L. B. Furstenau, M. K. Sott, and L. Mahlmann Kipper, "20 Years of Scientific Evolution of Cyber Security: a Science Mapping," 2020. [Online]. Available: https://www.researchgate.net/publication/340413661

DOI: https://doi.org/10.54216/JCIM.150218
Received: May 18, 2024 Revised: July 15, 2024 Accepted: November 06, 2024

[3] K. Cabaj, D. Domingos, Z. Kotulski, and A. Respício, "Cybersecurity education: evolution of the discipline and analysis of master programs," 2018.

[4] A. Golder, A. Bhat, and A. Raychowdhury, "Exploration into the Explainability of Neural Network Models for Power Side-Channel Analysis," in Proceedings of the ACM Great Lakes Symposium on VLSI, GLSVLSI, Association for Computing Machinery, Jun. 2022, pp. 59–64. doi: 10.1145/3526241.3530346.

[5] Y. Zhang, P. He, H. Gan, H. Zhang, and P. Fan, "Side-Channel Power Analysis Based on SA-SVM," Applied Sciences (Switzerland), vol. 13, no. 9, May 2023, doi: 10.3390/app13095671.

[6] A. P. Sayakkara and N. A. Le-Khac, "Electromagnetic Side-Channel Analysis for IoT Forensics: Challenges, Framework, and Datasets," IEEE Access, vol. 9, pp. 113585–113598, 2021, doi: 10.1109/ACCESS.2021.3104525.

[7] H. Tyralis, G. Papacharalampous, and A. Langousis, "A brief review of random forests for water scientists and practitioners and their recent history in water resources," Water (Switzerland), vol. 11, no. 5. MDPI AG, May 01, 2019. doi: 10.3390/w11050910.

[8] M. Sheykhmousa, M. Mahdianpari, H. Ghanbari, F. Mohammadimanesh, P. Ghamisi, and S. Homayouni, "Support Vector Machine versus Random Forest for Remote Sensing Image Classification: A Meta-Analysis and Systematic Review," IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 13. Institute of Electrical and Electronics Engineers Inc., pp. 6308–6325, 2020. doi: 10.1109/JSTARS.2020.3026724.

[9] L. Masure, C. Dumas, and E. Prouff, "A comprehensive study of deep learning for side-channel analysis," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2020, no. 1, pp. 348–375, 2020, doi: 10.13154/tches.v2020.i1.348-375.

[10] A. V. Krasovsky and E. A. Maro, "Actual and historical state of side channel attacks theory," in ACM International Conference Proceeding Series, Association for Computing Machinery, Sep. 2019. doi: 10.1145/3357613.3357627.

[11] M. Randolph and W. Diehl, "Power side-channel attack analysis: A review of 20 years of study for the layman," Cryptography, vol. 4, no. 2. MDPI AG, pp. 1–33, Jun. 01, 2020. doi: 10.3390/cryptography4020015.

[12] H. A. Khan et al., "IDEA: Intrusion Detection through Electromagnetic-Signal Analysis for Critical Embedded and Cyber-Physical Systems," IEEE Trans Dependable Secure Comput, vol. 18, no. 3, pp. 1150–1163, May 2021, doi: 10.1109/TDSC.2019.2932736

[13] N. Prates, A. Vergutz, R. T. MacEdo, A. Santos, and M. Nogueira, "A Defense Mechanism for Timing-based Side-Channel Attacks on IoT Traffic," in 2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings, Institute of Electrical and Electronics Engineers Inc., Dec. 2020. doi: 10.1109/GLOBECOM42002.2020.9322070.

[14] I. Shumailov, L. Simon, J. Yan, and R. Anderson, "Hearing your touch: A new acoustic side channel on smartphones," Mar. 2019, [Online]. Available: http://arxiv.org/abs/1903.11137

[15] Proceedings of the 23rd Conference on Design, Automation and Test in Europe. EDA Consortium, 2020.

[16] A. Dubey, R. Cammarota, and A. Aysu, "MaskedNet: The First Hardware Inference Engine Aiming Power Side-Channel Protection," Oct. 2019, [Online]. Available: http://arxiv.org/abs/1910.13063

[17] Y. Yao, P. Kiaei, R. Singh, S. Tajik, and P. Schaumont, "Programmable RO (PRO): A Multipurpose Countermeasure against Side-channel and Fault Injection Attack," Jun. 2021, [Online]. Available: http://arxiv.org/abs/2106.13784

[18] H. A. Khan, N. Sehatbakhsh, L. N. Nguyen, M. Prvulovic, and A. Zajić, "Malware Detection in Embedded Systems Using Neural Network Model for Electromagnetic Side-Channel Signals," Journal of Hardware and Systems Security, vol. 3, no. 4, pp. 305–318, Dec. 2019, doi: 10.1007/s41635-019-00074-w.

[19] J. He, Y. Liu, Y. Yuan, K. Hu, X. Xia, and Y. Zhao, "Golden chip free Trojan detection leveraging electromagnetic side channel fingerprinting," 2019, doi: 10.1109/MDT.

[20] N. Sehatbakhsh et al., "REMOTE: Robust External Malware Detection Framework by Using Electromagnetic Signals."

[21] Applied Computer Security Associates and Association for Computing Machinery, ACSAC 2021 : 37th Annual Computer Security Applications Conference : proceedings : Virtual Conference, 6-10 December 2021.

[22] Q. Le, L. Miralles-Pechuán, A. Sayakkara, N. A. Le-Khac, and M. Scanlon, "Identifying Internet of Things software activities using deep learning-based electromagnetic side-channel analysis," Forensic Science International: Digital Investigation, vol. 39, Dec. 2021, doi: 10.1016/j.fsidi.2021.301308.

DOI: https://doi.org/10.54216/JCIM.150218
Received: May 18, 2024 Revised: July 15, 2024 Accepted: November 06, 2024

[23] A. Sayakkara, N. A. Le-Khac, and M. Scanlon, "Leveraging Electromagnetic Side-Channel Analysis for the Investigation of IoT Devices," Digit Investig, vol. 29, pp. S94–S103, Jul. 2019, doi: 10.1016/j.diin.2019.04.012.

[24] N. Chawla, A. Singh, M. Kar, and S. Mukhopadhyay, "Application Inference using Machine Learning based Side Channel Analysis," Jul. 2019, [Online]. Available: http://arxiv.org/abs/1907.04428

[25] M. A. Bergstedt, "AFIT Scholar AFIT Scholar Malware Detection Using Electromagnetic Side-Channel Analysis Malware Detection Using Electromagnetic Side-Channel Analysis." [Online]. Available: https://scholar.afit.edu/etd/5316

[26] M. M. Khalifa, O. N. Ucan, and K. M. A. Alheeti, "Supervised Machine Learning to Enhance Security in Mobile Ad Hoc Networks," in Proceedings - International Conference on Developments in eSystems Engineering, DeSE, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 493–498. doi: 10.1109/DESE54285.2021.9719511.

[27] F. S. Mubarek, S. A. Aliesawi, K. M. A. Alheeti, and N. M. Alfahad, "Urban-AODV: an improved AODV protocol for vehicular ad-hoc networks in urban environment," Int. J. Eng. Technol., vol. 7, no. 4, pp. 3030–3036, 2018.

[28] S. R. Katte and K. E. Fernandez, "A Survey Report on Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis," Jul. 2023, [Online]. Available: http://arxiv.org/abs/2307.02012

[29] K. Ryan, "Return of the hidden number problem: A widespread and novel key extraction attack on ECDSA and DSA," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2019, no. 1, pp. 146–168, 2019, doi: 10.13154/tches.v2019.i1.146-168.

[30] M. S. Ibrahim Alsumaidaie, K. M. Ali Alheeti, and A. K. Alaloosy, "Intelligent Detection of Distributed Denial of Service Attacks: A Supervised Machine Learning and Ensemble Approach," Iraqi Journal for Computer Science and Mathematics, vol. 4, no. 3, pp. 12–24, 2023, doi: 10.52866/ijcsm.2023.02.03.002.

[31] A. K. Kareem, A. M. Shaban, A. A. Nafea, M. Aljanabi, S. A. S. Aliesawi, and M. Mal-Ani, "Detecting Routing Protocol Low Power and Lossy Network Attacks Using Machine Learning Techniques," in 2024 21st International Multi-Conference on Systems, Signals & Devices (SSD), 2024, pp. 57–62.

[32] S. A. Rafa, Z. M. Al-qfail, A. A. Nafea, S. F. Abd-hood, M. M. Al-Ani, and S. A. Alameri, "A Birds Species Detection Utilizing an Effective Hybrid Model," in 2024 21st International Multi-Conference on Systems, Signals & Devices (SSD), 2024, pp. 705–710.

[33] B. Al-Rami, K. M. A. Alheeti, W. M. Aldosari, S. M. Alshahrani, and S. M. Al-Abrez, "A New Classification Method for Drone-Based Crops in Smart Farming", Int. J. Interact. Mob. Technol., vol. 16, no. 09, pp. pp. 164–174, May 2022.

[34] H. J. Mohammed, A. A. Nafea, H. K. Almulla, S. A. S. Aliesawi, and M. M. Al-Ani, "An Effective Hybrid Model for Skin Cancer Detection Using Transfer Learning," in 2023 16th International Conference on Developments in eSystems Engineering (DeSE), 2023, pp. 840–845.

[35] A. A. Nafea et al., "Enhancing Student's Performance Classification Using Ensemble Modeling," Iraqi J. Comput. Sci. Math., vol. 4, no. 4, pp. 204–214, 2023.

[36] M. Sheykhmousa, M. Mahdianpari, H. Ghanbari, F. Mohammadimanesh, P. Ghamisi, and S. Homayouni, "Support Vector Machine versus Random Forest for Remote Sensing Image Classification: A Meta-Analysis and Systematic Review," IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 13. Institute of Electrical and Electronics Engineers Inc., pp. 6308–6325, 2020. doi: 10.1109/JSTARS.2020.3026724.

[37] Z. H. Abdaljabar, O. N. Ucan, and K. M. A. Alheeti, "An intrusion detection system for IoT using KNN and decision-tree based classification," in 2021 International conference of modern trends in information and communication technology industry (MTICTI), 2021, pp. 1–5.

[38] A. Sayakkara, N. A. Le-Khac, and M. Scanlon, "Leveraging Electromagnetic Side-Channel Analysis for the Investigation of IoT Devices," Digit Investig, vol. 29, pp. S94–S103, Jul. 2019, doi: 10.1016/j.diin.2019.04.012.

DOI: https://doi.org/10.54216/JCIM.150218
Received: May 18, 2024 Revised: July 15, 2024 Accepted: November 06, 2024