Non-Destructive Detection of Counterfeit Audio Amplifier Modules

Simone Carta
Department of Electrical and Electronic Engineering
University of Cagliari
Cagliari, Italy
simone.carta97@unica.it
ORCID: 0009-0009-1371-9851

Giovanna Mura
Department of Electrical and Electronic Engineering
University of Cagliari
Cagliari, Italy
gmura@diee.unica.it
ORCID: 0000-0002-8452-2345

***Abstract*—Counterfeiting in the electronics industry is an increasingly challenging issue to detect. The variety of counterfeit electronics adds complexity to the problem and underscores the need for advanced detection methods. Building on previous research, this paper presents a non-destructive detection approach that utilizes electrical measurements and machine learning algorithms, which can be trained in the field during operation. This method offers a cost-effective solution to this widespread issue, particularly for simple electronic devices. The approach, which has previously demonstrated its validity on standalone amplifiers, is now being refined and applied to commercial modules that incorporate the same components, further confirming its effectiveness.**

Keywords—counterfeit electronics, fake electronics, non-destructive detection, machine learning, counterfeit amplifiers modules

I. INTRODUCTION

Counterfeit electronics represent a growing threat to the reliability, safety, and security of modern electronic systems. These components may include fraudulent copies, imitations, or substitutes that are intentionally misrepresented as genuine. Typical examples include recycled, remarked, scrapped, or tampered parts.

Due to obsolescence or large procurement lead time, it may become necessary to turn to the so-called grey market, where availability and cost appear attractive, but quality and authenticity cannot be guaranteed. This creates a non-negligible probability of acquiring counterfeit devices.

In order to mitigate this risk, the development and adoption of reliable detection techniques is essential. While destructive approaches can reveal evidence of counterfeiting, they are costly and time-consuming. Non-destructive methods, by contrast, allow inspection and authentication without impairing device usability, making them especially valuable for in-line or large-scale testing. Such approaches are increasingly relevant for rapidly expanding sectors like the Internet of Things (IoT), where massive use of low-cost devices magnifies the consequences of counterfeit infiltration at the perception layer.

Building on an approach validated for standalone amplifiers, this work proposes an additional algorithm improvement and its application to commercial modules that use the same type of amplifier, thereby further confirming its effectiveness and easy scalability.

Project "NoDeCI- Non- Destructive Counterfeit Identification" funded by Regione Sardegna CUP: F23D23000130002

Moreover, it demonstrates the potential to provide a cost-effective, in-line screening solution, at least for relatively simple electronic devices and modules, thereby reducing the risk of counterfeit penetration into electronic systems.

II. RELATED WORK

To contrast the entering of counterfeit electronics into the supply chain, multiple techniques must be employed for detection. Both destructive and non-destructive methods have been standardized through joint efforts of industry and academia [1].

The identification process commonly begins with External Visual Inspection (EVI) [2, 3]. Additional common non-destructive methods include electrical characterization [3, 4], scanning acoustic microscopy [5, 6] and X-ray analysis [6]. Material analysis is also employed for counterfeits identification [7, 8]. Standard approaches can include destructive steps, such as decapsulation physical analysis, in which the die layout is examined to enable conclusive component identification [4, 6, 9].

Non-destructive approaches are preferable, and their necessity becomes particularly evident because, when acquiring components from unauthorized distributors, a few sample tests are insufficient to guarantee the authenticity of the entire lot, making blanket testing of all devices necessary.

In recent years, research has increasingly focused on the use of Machine Learning (ML) algorithms for the non-destructive detection of counterfeit electronics. Various approaches have been reported in the literature, employing, among others, optical imaging, electrical and electromagnetic testing, and physical or chemical characterization [10]. Although highly effective, physical analysis techniques are often time-consuming and require access to specialized laboratories or costly equipment. Conversely, electrical measurements can be a highly efficient way to authenticate electronic products when low-cost non-destructive acceptance testing is required.

Electrical measurements represent an important non-destructive step in the verification process, enabling the determination of whether the device is functionally conforming, detecting manufacturing or parametric defects, and providing conclusive evidence for identifying failure modes and mechanisms in failed devices [11-14]. Consequently, it represents a practical approach to detecting counterfeits [15], as it provides direct verification of the device's functionality and electrical characteristics and can ascribe differences in the layouts and processes. Electrical

testing includes DC/AC testing, functional testing, and burn-in.

Several studies have proposed the use of ML algorithms trained on electrical data for counterfeit device detection. Prior works [16-18] have primarily addressed the identification of aged devices, using both simulations and real measurements. Huang et al. [16] proposed a One-Class SVM trained exclusively on data from brand-new devices for classification purposes.

In order to propose a recycling-oriented approach, Zhang et al. [17], simulated aging in 45 nm technology, using path delay in digital circuits as a fingerprint for detecting recovered parts. Dogan et al. [18] focused on aging effects in FPGAs. An OC-SVM trained only on new devices successfully distinguished between original and recycled parts. Wang et al. [19] proposed a system identification method that exploits the effects of process variations on both PCB traces and ICs. The method leverages information from both the device and the board, but its applicability is limited to new designs or reconfigurable devices.

Differently from other works that focused on the employment of electrical characteristics for distinguishing original and recycled components, our previous work [20] compared the electrical characteristics of fake amplifiers acquired from unauthorized distributors with a vast set of original amplifiers acquired from an official distributor to train algorithms to detect counterfeit devices. This work extends the proposed non-destructive detection approach, by exploring additional algorithms and addressing the detection of counterfeit audio modules based on the LMxxx low-power audio amplifier. Moreover, we propose an approach in which models trained on features extracted from lower-cost stand-alone devices can also be employed to identify more complex modules where the device of interest is integrated within a circuit.

Numerous techniques have been proposed in the literature to detect counterfeit printed circuit board assemblies (PCBAs). Among the various approaches summarized in [21], the detection method discussed in this work emphasizes verifying the authenticity of key electronic components mounted on the board rather than assessing the entire Bill of Materials (BOM). This anti-counterfeiting strategy operates on the premise that if the key element is authentic, the PCBA is likely to be genuine as well.

However, this solution does have limitations; for example, it does not prevent authentic key components from being installed on counterfeit substrates [21]. Nonetheless, in cases involving commercial modules with different BOMs and layouts that share only a specific device and offer similar performance, this approach can provide a quick, low-cost method for at least minimal screening against counterfeits.

III. The Proposed Case Study: From Device to Module

The key electronic components under analysis are some LMxxx low-power audio amplifiers designed for low-voltage consumer applications and provided in a plastic dual-in-line package. Fraudulent imitations of the original devices have been detected though destructive physical analysis in previous works [22-24]. This kind of device is widely used in IoT applications, especially for signal conditioning in sound sensor-based systems or COTS speakers, as reported in [25-29]. Even if this amplifier is not the most critical element in these applications, it is crucial to recognize that even minor electronic components within an IoT system can significantly impact the overall application. If these components do not function correctly, are low-performing, or catastrophically fail, they can dramatically affect the mission. Therefore, attention to every aspect and hardware involved in the IoT application is essential for ensuring robust performance and high availability.

A. Key Components Measurement Setup

LMxxx have been electrically characterized by determining the quiescent supply current vs supply voltage characteristic and the frequency response. Quiescent current measurements have been performed via an Agilent B1500A semiconductor parameter analyser, short circuiting the input pins, according to the datasheet test conditions. Frequency response measurements have been performed by employing a TTi EB2025T Low-cost triple output bench power supply and a Digilent Analog Discovery 2, through the WaveForms Network Analyzer software. Both measurements have been performed in open condition and by connecting a 220 µF capacitor close to the power supply pin, while for the frequency response measurements a 22 µF bypass capacitor has been connected to pin 7, according to the instruction reported in the datasheet. Both current and gain values have been taken over an average of multiple measurements. The measurement setup schematics are shown in Fig. 1, while the characteristics for the set of original devices are shown in [20].

IV. Machine Learning Based Approach

By collecting electrical measurements from a large population of original and counterfeit devices (over 500 devices), several machine learning algorithms were explored to identify original and counterfeit devices. According to the manufacturer's datasheet information, three electrical characteristics were acquired for each device (quiescent supply current vs. the supply voltage, gain voltage and cut-off frequency). Among the characteristics listed in the datasheet, we focused on those for which the manufacturer specified typical test conditions. In addition to the three features, a further feature, the slope of the quiescent supply current vs. supply voltage characteristic, was included in the set.

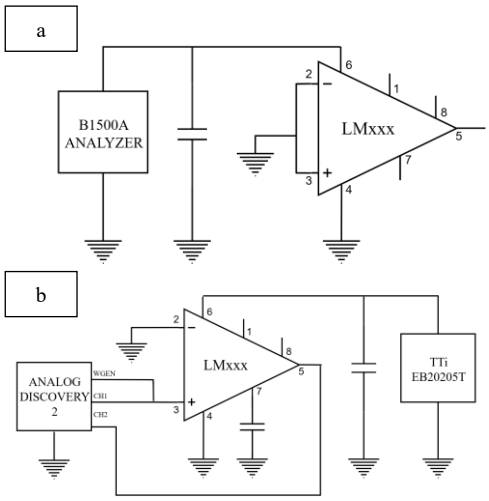


Fig. 1. Measurement setup for the quiescent supply current (a), and for the frequency response (b).

The analysis of the features' distribution and correlation enabled the second phase, which focused on the selection of the algorithms, which finally fell on both k-nearest neighbours (KNN) and linear support vector machine (SVM).

The study revealed that both algorithms perform excellently when four features are considered, reaching 100% in test output performance. Consequently, further sets of devices acquired from unauthorized distributors were verified with the best-performing algorithms. This additional verification showed that both algorithms well performed on the same kind of counterfeits used for the training phase, while for two kinds of new counterfeits, the output test was in contrast (one of the two classifiers recognized a fake counterfeit device as original). In these cases, a prudent strategy should prioritize the indication of "counterfeiting" given by at least one of the algorithms. The study demonstrated that machine learning-assisted electrical measurements can be a highly effective way to authenticate electronic products when a non-destructive verification is required.

Although the combined use of KNN and linear SVM classifiers has proven effective in identifying new counterfeit types, the inherent limitations of the selected classification models make them more prone to error, suggesting that more suitable classifiers could be employed. This limitation motivated the exploration of alternative classifiers better suited to the problem. In particular, an SVM with a Gaussian kernel (Radial Basis Function - RBF), given appropriate parameter tuning, can define a closed decision boundary enclosing the population of genuine devices, thereby improving the ability to recognize counterfeit types not included in training. In Table 1 the classification results on the test dataset are reported. Both three features (quiescent current, voltage gain, and cutoff frequency) and four features (the previous and the current slope) are used for training the SVM model with RBF kernel. Again, due to the perfect separation of data in the feature space, test results for the model trained with four features reach 100% performance.

For the three-feature model, the reported values are averages of the best-performing results obtained with the parameters yielding the highest accuracy, namely $\gamma = 1$ and $C \in \{0.1, 1, 10\}$. For the four-feature, model however, the test results always yield 100% performance for any pair of values used between $C \in \{0.1, 1, 10\}$ e $\gamma \in \{0.1, 1\}$. Considering the results reported in [20] on the classification of single devices, and repeating the test with the latter algorithm, all new kind of counterfeits are correctly classified.

TABLE I. SVM WITH RBF KERNEL, TEST PERFORMANCE COMPARISON.

Feat. number	Hyper-parameters	Accuracy	Precision	Recall	F-Score
3	$C \in \{0.1, 1, 10\}$ $\gamma = 1$	99.3%	98.7%	99.6%	99.1%
4	$C \in \{0.1, 1, 10\}$ $\gamma \in \{0.1, 1\}$	100%	100%	100%	100%

V. DETECTION OF COUNTERFEIT MODULES

The approach, which has previously demonstrated its validity on standalone devices, is now being applied to commercial modules that incorporate the same components, further confirming its effectiveness. In Fig. 3, four commercial modules are proposed. "W" and "Y" type mounted a through-hole version of the LMxxx, "X" and "Z" type mounted a surface-mount-device version one.

The goal is to identify the amplifiers in a non-destructive way. However, the electrical features considered for determining the authenticity of standalone devices, such as quiescent current or voltage gain, are affected by the surrounding circuitry. Still, by processing the data appropriately and making minimal additional measurements, or adjusting the measurement conditions, it remains possible to identify and characterize the target device.

In Fig. 4, the schematics of the audio modules are shown. Further details on the measurements carried out on the modules are provided below.

In both "X" and "Y" modules, an LED - resistor series is connected between the power supply and ground pins. This series draws a current comparable to that absorbed by the amplifier under quiescent conditions, thereby affecting DC measurements taken through the module connectors.

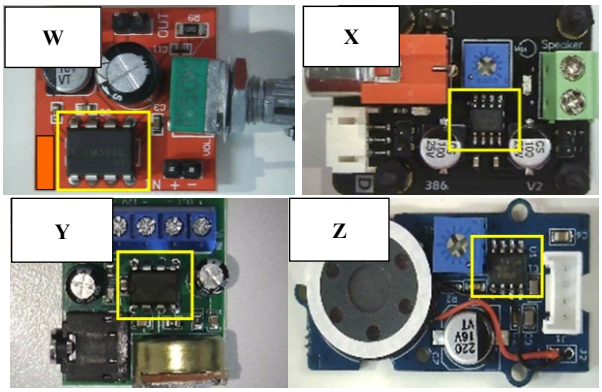
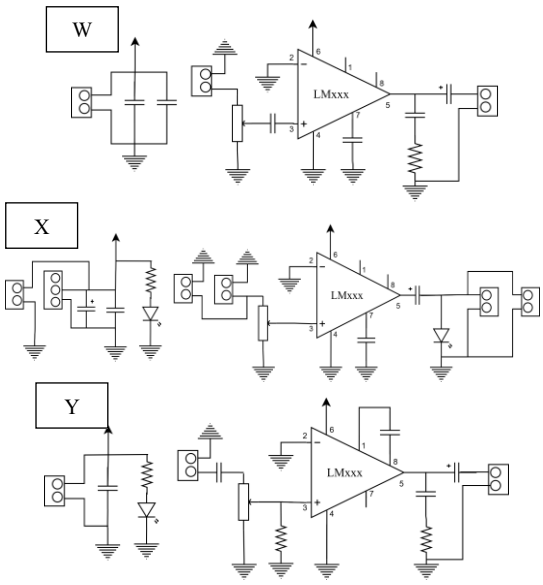


Fig. 3. Commercial audio amplifier modules. The LMxxx is yellow marked.



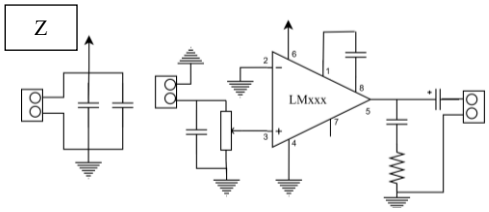


Fig. 4. Schematics for the commercial audio amplifier modules.

However, the LED current can be estimated by knowing the LED threshold voltage and the value of the series resistor. Both parameters can be obtained through point-to-point measurements on the module's components, allowing an estimation of the amplifier's quiescent current.

In both "Y" and "Z" modules, a gain capacitor is connected between pins 1 and 8, which increases the amplifier gain from 26 dB up to 46 dB (as specified in the datasheet). Under this scenario, gain can no longer be measured using the standard test condition (supply voltage of 6 V, frequency of 1 kHz). Nevertheless, since the amplifier exhibits a low-pass response, the expected gain can still be determined at a lower frequency (around 1 Hz), where the gain capacitor behaves as an open circuit and has no effect on the amplifier's gain.

The presence of the gain capacitor affects both gain and bandwidth measurements. While the gain can be directly measured by adjusting the test conditions, the bandwidth must be estimated. The estimation proceeded as follows: the frequency response of the amplifier can be modelled by a second-order transfer function. By adjusting the feedback pins, it is possible to vary the gain without altering the high-frequency behaviour. Therefore, the cutoff frequency was determined using an asymptotic construction, as the intersection of the low-frequency gain line with the –40 dB/decade line observed at high frequencies. Even if in the schematic of "Z" module the load is not represented, a speaker is embedded in the module, as can be seen in the "Z" module picture. To avoid the load effect on the frequency response, the speaker has been carefully desoldered from the board.

In Fig. 5, some scatter plots show, for the features of interest, the variations of the features positioning in the feature space before and after processing the data or changing the measurement conditions. For "W" module no additional processing is needed. The proposed machine learning approach, applied to the audio modules, is presented in Table 2. The modules are correctly classified. "X" and "Z" modules were acquired on the official market, so they are original. Module "W" and "Y" was purchased from a popular online broker. In principle, it is considered suspect and is now recognized as counterfeit, without the need for any further physical inspection. It further confirms the feasibility and effectiveness of the proposed approach.

V. Conclusion

This work presents a simple and cost-effective method for detecting counterfeit electronic amplifiers mounted on modules through electrical characterisation and machine learning algorithms. The study focuses on four commercial modules, where the amplifier is a key component. By making minimal additional measurements or adjusting the measurement conditions, it remains possible to characterise the amplifier easily.

TABLE II. ORIGINAL (O) AND COUNTERFEIT (C) CLASSIFICATION.

ML models	Module W	Module X	Module Y	Module Z
KNN	C	O	C	O
SVM linear	C	O	C	O
SVM RGB	C	O	C	O

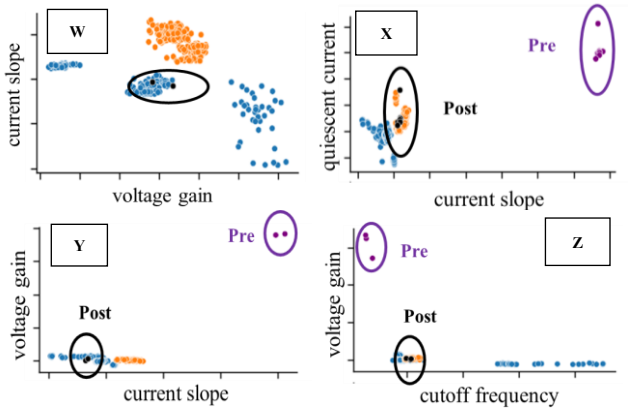


Fig. 5. Pre and post-processed results for "X", "Y" and "Z" modules and data point for "W" module. In violet, pre-processed data are converted to black, resulting in superimposition with the previous standalone originals (orange) for "X" and "Z", or with counterfeit devices (blue) for "Y", as well for "W" module.

A support vector machine (SVM) with a Gaussian kernel classifier was validated, showing enhanced performance compared to the previously proposed k-nearest neighbours (KNN) and linear SVM classifiers in accurately identifying new types of counterfeit devices. This SVM model was then applied to authenticate the commercial modules.

The results indicate that this methodology can be effectively utilized in industrial settings, where algorithms can be trained on lower-cost measurements obtained from standalone devices and subsequently employed for the direct verification of the same kind of device when mounted in more complex modules.

Acknowledgment

The Authors are in debt with Alessandro Urru (Nurjana Technologies Srl) for fruitful discussions.

References

[1] SAE International, AS6171A: Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts.

[2] B. Sood, D. Das, and M. Pecht, "Screening for counterfeit electronic parts," J. Mater. Sci.: Mater. Electron., vol. 22, pp. 1511-1522, 2011.

[3] A. Shrivastava, M. H. Azarian, C. Morillo, B. Sood, and M. Pecht, "Detection and reliability risks of counterfeit electrolytic capacitors," IEEE Trans. Reliab., vol. 63, no. 2, pp. 468-479, 2014.

[4] G. Mura, "Reliability concerns from the gray market", Microelectron. Reliab., vol. 88-90, pp. 26-30, 2018.

[5] Y. Qiu, S. Zhang, Z. Chen, Y. Li, and M. Jiang, "Counterfeit identification method of plastic encapsulated microcircuits using scanning acoustic microscope," J. Phys.: Conf. Ser., vol. 1074, no. 1, 2018.

[6] Y. L. Wang, X. Kuang, C. Huang, and S. P. Li, "Case studied of failure threat caused by counterfeit plastic encapsulated microcircuits," Proc. of the 20th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), Suzhou, China, 2013, pp. 574-577.

[7] M. Navrátil, P. Neumann, and V. Křesálek, “Advanced microscopic techniques used for integrated circuits authenticity analysis,” J. Phys.: Conf. Ser., vol. 1065, no. 10, p. 102015, Aug. 2018.

[8] A. Shrivastava, and M. Pecht, “Counterfeit capacitors in the supply chain,” J. Mater. Sci.: Mater. Electron., vol. 25, pp. 645-652, Mar. 2014.

[9] Y. Hong, “Detection of a counterfeit OTA device and certification of a replacement source,” Proc. of International Symposium for Testing and Failure Analysis (ISTFA), 2011, vol. 38268, pp. 234-237.

[10] S. U. Shankar, and P. Kalpana, “A review on machine learning based counterfeit integrated circuit detection,” Eng. Res. Express, vol. 5, p. 042002, 2023.

[11] M.J. Deen, and F. Pascal, “Electrical characterization of semiconductor materials and devices,” in: “Springer handbook of electronic and photonic materials,” S. Kasap, and P. Capper, Springer, Cham, 2017.

[12] A. Grochowski, D. Bhattacharya, T. R. Viswanathan and K. Laker, “Integrated circuit testing for quality assurance in manufacturing: history, current status, and future trends,” IEEE Trans. Circuits Syst. II: Analog and Digital Signal Process., vol. 44, no. 8, pp. 610-633, Aug. 1997.

[13] G. Mura, M. Vanzi, G. Marcello, and R. Cao, “The role of the optical trans-characteristics in laser diode analysis,” Microelectron. Reliab., vol. 53, no. 9–11, pp. 1538-1542, 2013.

[14] M. Vanzi et al., “Extended modal gain measurement in DFB laser diodes,” IEEE Photonics Technol. Lett., vol. 29, no. 2, pp. 197-200, 2017.

[15] M. Tehranipoor, U. Guin, and D. Forte, “Electrical tests for counterfeit detection,” in: “Counterfeit integrated circuits,” Springer, Cham, 2015.

[16] K. Huang, Y. Liu, N. Korolija, J. M. Carulli, and Y. Makris, “Recycled IC detection based on statistical methods,” IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., vol. 34, no. 6, pp. 947-960, 2015.

[17] X. Zhang, K. Xiao, and M. M. Tehranipoor, “Path-delay fingerprinting for identification of recovered ICs,” Proc. of IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Austin, TX, USA, 2012, pp. 13-18.

[18] H. Dogan, D. Forte, and M. M. Tehranipoor, “Aging analysis for recycled FPGA detection,” Proc. of IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Amsterdam, Netherlands, Oct. 2014, pp. 171-176.

[19] X. Wang, Y. Han, and M. Tehranipoor, "System-level counterfeit detection using on-chip ring oscillator array," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 27, no. 12, pp. 2884-2896, 2019.

[20] S. Carta, A. Urru, M. Musa, P. Andronico, and G. Mura, “Electronics authentication using electrical measurements and machine learning,” Microelectron. Reliab., vol. 168, p. 115652, May 2025.

[21] G. Mura et al., "Detecting counterfeit electronic circuits: the effect of PCB thickness and dielectric permittivity on the electromagnetic fingerprint," IEEE Sensors J., vol. 25, no. 17, pp. 33849-33858, 2025.

[22] G. Mura, R. Murru, and G. Martines, “Analysis of counterfeit electronics,” Microelectron. Reliab., vol. 114, p. 11379, Nov. 2020.

[23] G. Mura, R. Murru, and G. Martines, “Analysis of fake amplifiers,” Proc. of IEEE Int. Conference on Microelectronics (MIEL), Nis, Serbia, 2021, pp. 131-134.

[24] G. Mura, S. Carta, P. C. Ricci, and G. Martines, “Electronic components authentication via physical analysis,” Proc. of IEEE Int. Conference on Microelectronics (MIEL), Nis, Serbia, 2023, pp. 1-4.

[25] J. E. Rivadeneira et al. “CONFLUENCE: an integration model for human-in-the-loop IoT privacy-preserving solutions toward sustainability in a smart city,” IEEE Internet of Things J., vol. 11, no. 5, pp. 8690-8714, Mar. 2024.

[26] P. Jafarzadeh, F. Farahnakian, J. P. Paalassalo, and O. Eerola, “IoT-based household energy consumption prediction using machine learning,” EAI/Springer Innovations in Communication and Computing. Springer, Cham., pp. 137-152, 2021.

[27] E. Babu, J. Francis, E. Thomas, R. Cherian, and S. S. Sunandhan, “Predictive analysis of induction motor using current, vibration and acoustic signals,” Proc. of Int. Conference on Power Electronics & IoT Appl. in Renewable Energy and its Control (PARC), 2022, pp. 1-7.

[28] A. Maity, and I. S. Misra, “Prototype design of an IoT enabled cost-efficient portable heart-health data acquisition system,” Proc. of IEEE Calcutta Conference (CALCON), 2020, pp. 137-141.

[29] Y. Zhang, and K. Rasmussen, “Detection of electromagnetic signal injection attacks on actuator systems,” Proc. of Int. Symposium on Research in Attacks, Intrusions and Defenses, 2022, pp. 171-184.