Machine Learning-Based Autonomous Physical Security Defences

[1]Dr Subba Rao Polamurı, [2] Mr Knvpsb Ramesh, [3]K D Srıhıtha, [4]M Srıdevı , [5]M. Sangeetha, [6]A Yv M Gurudatta

[1,2,3,4,5,6]Department of CSE, BVC Engineering College, Odalarevu, A.P,India
[*1]psr.subbu546@gmail.com
[2]ramesh.kb17@gmail.com

Abstract. Nearly 50 billion linked devices by 2025 will make physical entry to the target system much easier for attackers. The proliferation of embedded devices in mission-critical infrastructure and industrial control systems, as well as the existence of the Internet of Battlefield Things (IoBT), heighten this risk. Existing anti-tamper designs have limited efficacy in preventing specific types of attacks and rely on predetermined responses to detect manipulation, which can undermine system reliability. More covert attacks are now feasible thanks to new physical inspection technology. Therefore, there is an immediate need for improved defences that can endure the anticipated rise in hostile capabilities for a considerable amount of time. If we want to take physical security to the next level, this study suggests building a smart anti-tamper with machine learning algorithms. It employs a number of analytical frameworks, one of which can distinguish between normal functioning, known attack vectors, and unusual behaviour. To further aid in the reduction of false alarms and enhancement of operating time, the system has a tiered reaction mechanism as well as a recovery strategy.

Keywords: Internet-of-Battlefield Things (IoBT), Machine Learning Algorithms, Stealthier attacks, Intelligent anti-tamper, Physical attacks

1.Introduction

It has These days, gadgets just can't survive being physically attacked in hazardous environments. This is a major worry due to the increasing number of BMSs and IoBTs, which stands for the Internet of Battlefield Things. The worldwide market for these systems is expected to surpass US$26 billion by 2027 [1]. One example of a system of this class is a UAV, or unmanned autonomous vehicle. With autonomous coordination, activities in enemy zones can be conducted safely, without putting human lives in danger, because it is more precise, durable, and reliable than humans. For unmanned aerial vehicles (UAVs) to be useful in military operations, they must be able to fulfil demanding standards for reliability, safety, and longevity. One of the most important things these systems need in terms of security is "physical end-point protection," according to a study by the Norwegian Defence Research Establishment (FFI) [2]. Physical security is crucial for many commercial applications, including Pay-Tv, military network encryption equipment, and payment terminals [3].

2.Literature Survey

K. R. Madhavi et al. (eds.), *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024)*, Advances in Computer Science Research 112,
https://doi.org/10.2991/978-94-6463-471-6_118

These shields encase the whole system, rendering it unusable for drilling, etching, or probing. For instance, in [8], the authors propose a tamper-proof envelope that would encase the system in a multi-layer mesh of electrical traces.. Typically, systems designed to prevent tampering include three main components: tamper detection (such as sensors that can detect attempts at tampering), tamper evidence (such as a log that records when a tamper event occurs), and tamper response (the steps implemented to safeguard the system once an attack is detected) [4]. Many different kinds of sensors can be employed to detect tampering; they include probe sensors, light, voltage, pressure, and temperature sensors, each of which can identify a distinct attack. If the device's enclosure has been broken or if a specific module has been moved, the switches can detect it. It is not common practise to employ defined procedures at the chip level due to the high cost and time required to manufacture integrated circuits [6]. Consequently, a lockable cabinet is used to house extremely sensitive devices that contain several chips [6, 7]. These shields encase the whole system, rendering it unusable for drilling, etching, or probing. For instance, in [8], the authors propose a tamper-proof envelope that would encase the system in a multi-layer mesh of electrical traces.. To start with, the monitoring circuitry is sensitive to static signals, thus a hacker may theoretically evade detection by artificially inducing the necessary voltage. The deterministic tamper response can potentially hinder the device's functionality; for example, if the tracks are accidentally damaged, it will trigger a needless reaction that removes CSP and stops the device from working.

The proposed solution to this problem is to use attack detection algorithms based on machine learning. These algorithms include the following: One Class Support Vector Machine, Isolation Forest, K-Nearest Neighbour, Local Outlier Factor, Histogram-Based Outlier, and Cluster-Based Outlier Factor. Following training on sensor data, all data will be assigned a label of either 1 (normal behaviour) or -1 (attack behaviour) to reflect the algorithms' performance. Without building any physical equipment, we may use machine learning techniques to predict when any kind of data manipulation will occur in the sensors. For example, we know that the average range of sensor temperatures is 20–31, so if a sensor reading drops below 20 or rises above 40, it will be considered an attack.

3.System Overview

SVM: A supervised machine learning approach, Support Vector Machine (SVM) is applicable to problems involving regression as well as classification. But categorization difficulties are where it really shines.

K-NN: One of the most basic ML algorithms, K-Nearest Neighbour relies on the supervised learning method.When a new data point is compared to the existing data, the K-NN algorithm sorts it according to how similar it is. What this implies is that the K-NN algorithm can readily sort newly-arrived data into a suitable category.

Decision Tree algorithm: Using only a few of basic decision rules deduced from the data, the objective is to build a model that can forecast the target outcome. Readability, solve-ability, and application to problems with several outputs are some of the advantages of this method.

Random forest algorithm: This approach randomly splits each simple decision tree using a subset of the available criteria for tree splits. Furthermore, the data needed to train the trees is selected randomly. In a random forest, when training, each tree uses a distinct subset of the whole data set.

Bagging classifier: To train several models, an ensemble method called "bagging" uses bootstrap resampling to generate numerous subsets of the training data. Overfitting can be mitigated and model performance improved by using the Bagging Classifier on a high-variance base classifier.

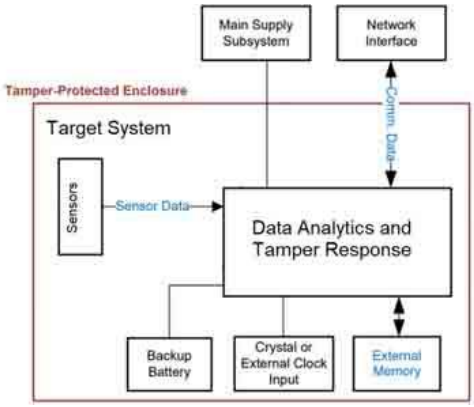

Fig 1. architecture of the proposed defense system.

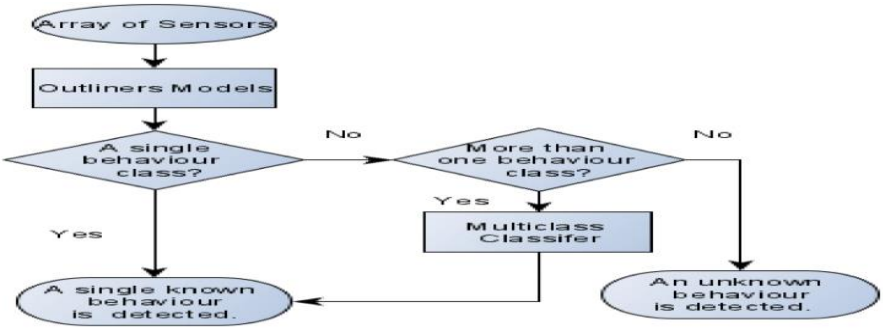

Fig 2: Principles of the proposed anomaly detection/classification scheme.

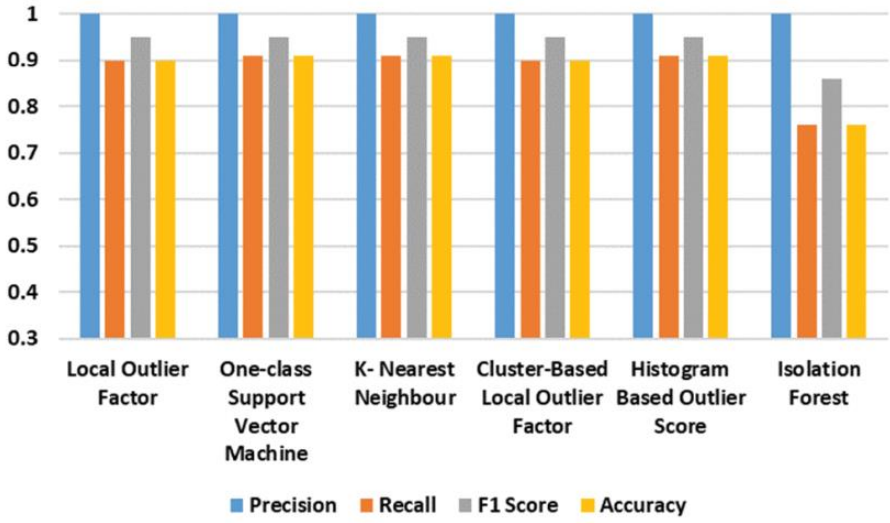

Fig 3 Performance comparison of outlier algorithms or normal behaviour indoor using a test set

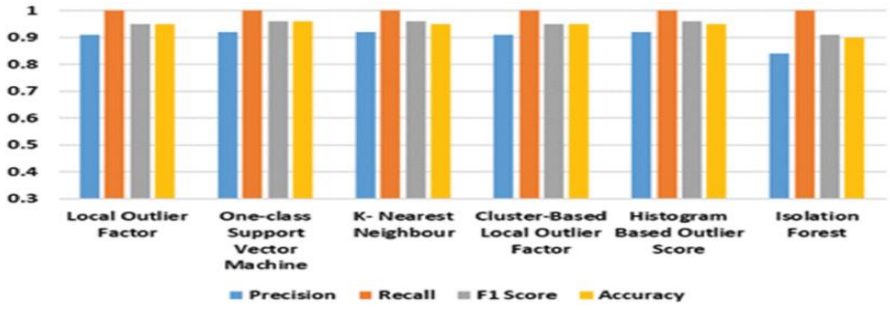

Fig 4: Performance comparison of outlier algorithms for normal behaviour indoors using a test set containing a mixture of normal and tamper data

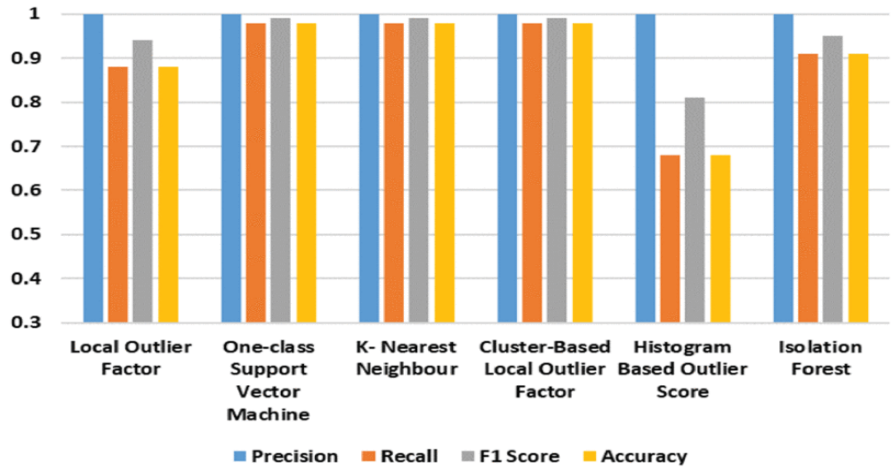

Fig 5: Performance comparison of outlier algorithms for the heating attack using a test set containing a mixture of normal and tamper data

4. Conclusion

The need for anti-tamper design techniques, which safeguard electronics systems deployed in dangerous or physically exposed environments, has grown substantially due to the expansion of the Internet of Battlefield Things (IoBT) and the growing dependence on embedded devices in critical infrastructure and industrial control systems.An autonomous anti-tamper design utilising machine learning methods was proposed in this paper. Using an analytical system that can detect and classify numerous types of behaviours is the essence of this technique.

.

References

[1] Research and Markets. (2020). Battlefield Management Systems Market to 2027—Global Analysis and Forecast by Component; System; Application. [Online]. Available: https://www.researchandmarkets.com/ reports/4987798/battlefield-management-systems-market-to-2027#rela0- 4897475

[2] S. B. F. Mancini, R. Fardal, J. H. Wiik, B. Greve, L. E. Olsen, and B. Bjerketveit,

‘‘Information security for unmanned and autonomous vehicles—Main challenges and relevant operational concepts,’’ Norwegian Defence Res. Establishment, Kjeller, Norway, FFI Rep.

19/00888, 2019. [Online]. Available: https://publications.ffi.no/nb/component/jcar/asset/dspace:7002/1772319.pdf

[3] A. Paulshus, ‘‘Anti-tamper and cryptography in pay-TV—Lessons learned,’’ presented at
the AVT-337 Res. Workshop Anti-Tamper Protective Syst. NATO Oper., 2021.
[4] J. Grand, ‘‘Practical secure hardware design for embedded systems,’’ in Proc. Embedded Syst. Conf., San Francisco, CA, USA, 2004, pp. 1–25.
[5] S. H. Weingart, ‘‘Physical security devices for computer subsystems: A survey of attacks and defenses,’’ in Cryptographic Hardware and Embedded Systems—CHES 2000. Berlin, Germany: 2000, pp. 302–317.
[6] J. Obermaier and V. Immler, ‘‘The past, present, and future of physical security enclosures: From battery-backed monitoring to PUF-based inherent security and beyond,’’ J. Hardw. Syst.
Secur., vol. 2, no. 4, pp. 289–296, Dec. 2018.
[7] CryptoServer Se-Series Gen2 Security Policy (Compliant to FIPS 140-2 Level and 3), UTIMACO, Aachen, Germany, 2018.
[8] P. Isaacs, T. Morris, Jr., M. J. Fisher, and K. Cuthbert, ‘‘Tamper proof, tamper evident encryption technology,’’ presented at the Pan Pacific Symp. (SMTA), 2013.
[9] V. Immler, J. Obermaier, M. König, M. Hiller, and G. Sig, ‘‘B-TREPID: Batteryless tamper-
resistant envelope with a PUF and integrity detection,’’ in Proc. IEEE Int. Symp. Hardw.
Oriented Secur. Trust (HOST), Apr. 2018, pp. 49–56.
[10] B. Halak, Physically Unclonable Functions: From Basic Design Principles to Advanced Hardware Security Applications. Cham, Switzerland: Springer, 2018.
[11] C. Bao, D. Forte, and A. Srivastava, ‘‘On reverse engineering-based hardware Trojan
detection,’’ IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 35, no. 1, pp. 49–57, Jan. 2016.
[12] C. Dong, Y. Liu, J. Chen, X. Liu, W. Guo, and Y. Chen, ‘‘An unsupervised detection approach for hardware trojans,’’ IEEE Access, vol. 8, pp. 158169–158183, 2020.
[13] Z. Huang, Q. Wang, Y. Chen, and X. Jiang, ‘‘A survey on machine learning against hardware trojan attacks: Recent advances and challenges,’’ IEEE Access, vol. 8, pp. 10796–10826, 2020.
[14] Y. Jin, D. Maliuk, and Y. Makris, ‘‘A post-deployment IC trust evaluation architecture,’’ in Proc. IEEE 19th Int. On-Line Test. Symp. (IOLTS), Jul. 2013, pp. 224–225.
[15] K. Huang, J. M. Carulli, and Y. Makris, ‘‘Parametric counterfeit IC detection via support vector machines,’’ in Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT), Oct. 2012, pp. 7–12.
[16] A. Stern, U. Botero, F. Rahman, D. Forte, and M. Tehranipoor, ‘‘EMFORCED: EM-based fingerprinting framework for remarked and cloned counterfeit IC detection using machine learning classification,’’ IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 28, no. 2, pp. 363–375, Feb. 2020.
[17] B. Halak, Ageing of Integrated Circuits: Causes, Effects and Mitigation Techniques. Cham, Switzerland: Springer, 2020.
[18] C. H. B. Halak, S. Fathir, N. Kit, R. Raymonde, and H. Vincent, ‘‘On the feasibility of usingmachine learning for an enhanced physical security of embedded devices,’’ presented at the IEEE SMARTTECH, May 2022, pp. 206–2011.
[19] R. J. Anderson, ‘‘Physical tamper resistance,’’ in Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. Hoboken, NJ, USA: Wiley, 2008, pp. 483– 521.

[20] E. Johansson, ‘‘Tamper protection for cryptographic hardware: A survey and analysis of state-of- the-art tamper protection for communication devices handling cryptographic keys,’’Dept. Electr. Eng., Linkoping Univ., Linköping, Sweden, Tech. Rep. ISRN: LIU-ISY/LITH-EX-A–20/5306– SE, 2020.