International Journal for Modern Trends in Science and Technology
Volume 12, Issue 03, pages 240-248.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue03.html
DOI: https://doi.org/10.5281/zenodo.18901069

A Dual-Layer Hardware Trojan Detection Framework using Area-Optimized AES and Real-Time IP Traffic Analysis

B. Hemavathi[1], N. Venkata Laxmi[2], N. Tri Sai Naga Vardhan[2], K. Narendra[2]

Department of ECE, Godavari Global University, Rajamahendravaram, INDIA.
Department of ECE, Godavari Institute of Engineering & Technology (A), Rajamahendravaram, INDIA.

To Cite this Article
B. Hemavathi, N. Venkata Laxmi, N. Tri Sai Naga Vardhan & K. Narendra (2026). A Dual-Layer Hardware Trojan Detection Framework using Area-Optimized AES and Real-Time IP Traffic Analysis, 12(03), 240-248. https://doi.org/10.5281/zenodo.18901069

Article Info
Received: 28 January 2026; Revised: 26 February 2026; Accepted: 02 March 2026.

KEYWORDS

Hardware Trojan Found, Area Transfer AES, Two-layer Security, IP Traffic, Attack Identification, Trojan Type, Network Immoralization, Email Earning System, Cybersecurity.

ABSTRACT

Hardware Trojans are an extensive repercussion to contemporary built-in circuits and cyber-physical frameworks as they bring about rogue changes that affect confidentiality, integrity and availability. In an effort to reduce this challenge, this paper presents a dual-layer Trojan detection framework which combines both hardware optimization based and software IP traffic analysis and alerting. An Area Reduction Advanced Encryption Standard (AR-AES) architecture is used at the hardware layer to reduce the use of logic with preservation of cryptographic strength. The signs used to access deviations of expected area, power, or timing requirements are used to verify the possibility that a Trojan is inserted. At the software level, a real time IP traffic monitoring service is constantly examining the traffic sent to the network and deriving the attributes of the traffic, and determining the abnormal patterns of access like high request rates or the abnormal re-use of certain IP addresses. The suggested system takes place in two phases one of which is an Attack Detector which allows identifying the traffic as possible malicious or normal and the other is the Attack Identifier which further separates the Trojan activity detected. The system sends an email-based notification to the administrators, who can receive the alert information promptly upon detecting an anomalous behavior. Through effective cryptographic hardware analysis combined with smart network level monitoring, the suggested method will provide a strong, scalable and proactive security measure that will be able to detect both the hardware Trojans and network based attack vectors with a better accuracy and lower response time.

INTRODUCTION

The high rate of globalization of semiconductor products and the continued reuse of third-party intellectual property (IP) cores have greatly exposed contemporary integrated circuits (ICs) to malignant manipulation termed Hardware Trojans (HTs). Such Trojans can be introduced in the design, fabrication or creation or testing phase and can go inactive until activated resulting in information release, denial of service or system malfunction [1], [2]. Since they are stealthy and only require minimum hardware footprint, HTs present significant risk to the security, reliability, and trustworthiness of electronic systems implemented in critical applications.

In the last ten years, there have been comprehensive studies to identify HTs with the help of logic testing, side-channel analysis, and formal verification. The goal of logic testing method is to stimulate Trojan circuitry using specially designed test vectors and monitor deviant responses [3], [7], [8]. Although they work with some types of Trojan, such approaches frequently have low activation likelihood and low coverage, when used with infrequent Trojans [4], [6]. Moreover, the lack of golden reference model to third-party IP cores is a major drawback that makes detection based on logic to be extremely difficult [6].

The approaches that rely on side-channel analysis take advantage of the difference in power usage, timing, or electromagnetic emissions to detect trojan-induced events [5], [9], [11]. Though these methods have the ability of finding dormant Trojans without necessarily being triggered, the process variations, environmental noise and measurement uncertainty severely hamper the reliability of these techniques [10], [11]. The design of the advanced Trojan, like zero power and area footprint, has pushed even further to show the limitations of the old methods of side-channel [1].

To address these limitations, statistical and machine learning-based systems have been proposed to achieve better detection resilience when there is circuit behavior modeling and detection of outliers to the expected behavioral patterns [9], [13]. These techniques are better scaled and automated, but their performance is very sensitive to the quality of training data and feature selection, and can still have problems with strongly-optimized Trojan design [14].

Due to these shortcomings, the proposed work is based on a dual-layer Trojan detection system that combines hardware-level AES optimization based anomaly detection and software level IP traffic surveillance and automatic alerting. The proposed system allows improving the level of detection accuracy, the response time, and the provision of a proactive defense mechanism against hardware Trojans and network based attacks through a combination of cryptographic hardware analysis and automated classification of network traffic and real-time email notification. The objective of this integrated strategy is to enhance system reliability and cyber-physical system security in upcoming embedded and cyber-physical systems.

Problem Statement

Regardless of tremendous progress in detection of hardware Trojan, the current methods have a number of severe weaknesses. The logic testing-based techniques are usually ineffective in executing the stealthy or rarely executed Trojans and the side-channel analysis technique is very sensitive to process variations, environmental noise and inaccuracies in measurements. The latest Trojan layouts also circumvent detection because it creates imperceptible power, area and timing prints, making the conventional detectives useless.

Further, the latest methods used only deal with hardware-level analysis without the usage of software level and network level indications that could show predatory activity in the process of system usage. Hardware Trojans are commonly executed or used in practice by some kind of abnormal network usage, like unauthorized access incurred or overload of the system by certain IP addresses. Absence of embedded hardware-software security systems translates to poor timeliness of detection, situal awareness, as well as responding to the events.

Objectives of the Research

The main goal of the study is to construct an area-constrained Advanced Encryption Standard (AES) architecture that maintains the level of cryptography and allows detecting anomalies in hardware that occurs by Trojan insertion. Secondly, a two-layer detection system is designed, which involves the attack detection stage

and the attack identification stage, to determine the malicious behavior correctly. The offered system also real-time IP traffic monitoring that helps to detect abnormal access patterns that might be referred to as Trojan activation or unauthorized system usage. An automated email-based alerting system is installed so as to facilitate a quick reaction in case of identifying threats. The proposed method will supplement the accuracy of the detection response by correlating the hardware-level indicators of anomalies with the network-level analysis of the traffic, and greatly decrease the average response time.

This work has made initial contributions which are as follows:

(a) A Trojan detection architecture with both hardware-based cryptographic anomaly detection and software-based network traffic analysis.

(b) An Area Reduction AES (AR-AES)-based detection mechanism which relies on differences in the use of resources to help in detection of stealthy hardware Trojan.

(c) Two-step classification system that is composed of an Attack Detector and an Attack Identifier to accurately classify Trojan.

(d) An IP real-time stalker module which detects high request rates and uncharacteristic access patterns.

(e) Automated email notification system that allows proactive response of security and less latency of mitigation.

In this paper, a dual layer security framework is introduced that has the advantage of overcoming the shortcomings of the traditional hardware Trojan detection technology. The protection against stealthy Trojan insertions, as well as network-based attack vectors, has been completely offered by the proposed approach, combining power-efficient AES-based hardware anomaly detection with smart IP traffic monitoring. A combination of a 2-step model of detection and identification, and automatic email alerts facilitates the accuracy of detection and response in time, thus rendering the proposed system an appropriate choice when it comes to utilizing secure embedded and cyber-physical features.

The rest of this paper will be structured in the following way. In section II, a review of current hardware Trojan detection methods and capabilities is conducted on a comprehensive basis. The proposed dual-layer Trojan detection framework (that is, the optimized AES architecture and the IP monitoring mechanism) is outlined in section III. The experimental setup, performance metrics and results analysis are discussed in Section IV. Section V summarizes the paper and provides directions in which future research can be taken.

LITERATURE SURVEY

Globalization in the manufacture of semiconductor integrated circuits and dependency on third-party intellectual property (IP) cores have led to Hardware Trojans (HTs) becoming an important security issue in contemporary integrated circuits. In recent years, due to the overwhelming amount of research has been conducted on the design, insertion, detection and mitigation of HTs, in logic testing, side-channel analysis, statistical learning and cryptographic methods.

TrojanZero, a new category of stealthy hardware Trojans that ensures zero power and area overhead was presented by Abbassi et al. to achieve bypassing of the conventional side-channel detection techniques due to the use of switching activity awareness [1]. It is a work, which highlighted weaknesses of traditional power- and area-based Trojan detection methods. Xiao et al. conducted broad survey on the research on hardware Trojan in ten years and classified Trojan models, turn-on methods and turn-off methods as well as detection schemes; they argued that dimension-wide detection frameworks must be adopted [2].

Bhasin and Regazzoni introduced a detailed overview of hardware Trojan detection methods such as logic testing, side-channel analysis, run-time monitoring, and formal verification, and also talked about their weaknesses and limitations when applied in the real world [3]. According to Saha et al., a better test pattern generation method was suggested with the help of genetic algorithm and Boolean satisfiability, increase the chances of Trojan activation during testing [4].

Side-channel analysis has been popularly investigated in detecting Trojan horses. Narasimhan et al. showed that power, delay and electromagnetic emissions can be maximally combined to enhance detection accuracy many times higher than using single parameters [5]. Zhang and Tehranipoor explored the problems of detecting Trojan attacks in third-party digital IP cores, which discussed the challenge of getting

golden reference record and suggested trust evaluation methods [6].

The detection methods based on logic testing were also studied by Bazzazi et al. who could prove that malicious logic embedded as hardware Trojans could be detected with a well-crafted test vectors [7]. Govindan and Chakraborty extended the logic testing approaches and talked about their place in formal Trojan detection in secure hardware design processes [8].

Another effective method that has been utilized in detecting the Trojan induced aberrations is statistical methods. Chakraborty et al. proposed a statistical search MERO framework that identifies hardware Trojans as changes by modeling circuit behavior changes and determining an anomaly against the predicted distribution [9]. Nevertheless, Di Natale and Dupuis raised some doubts about the consistency of side-channel analysis in the presence of process variation, demonstrating that presence of environmental noise can severely affect the performance of detection [10].

Rad et al. conducted sensitivity analysis on the power-based Trojan detection methods and showed how they are susceptible to both process and environmental variations that can be used to cover Trojan signatures [11]. Potkonjak et al. introduced techniques of characterizing gate-level because this method would identify HTs through the monitoring of parametric deviations that arose in the course of fabrication [12].

In the effort to curb the problem of scalability and robustness, Chen et al. suggested a general method involving statistical learning algorithms to detect Trojan hardware, which can be used to separate Trojan-free and Trojan-infected circuits automatically [13]. Haider et al. created the state-of-the-art with the implementation of an extended range of detection approaches and their comparison on various Trojan benchmarks [14].

A number of publications have dwelled on Trojan design and modeling in order to gain a clearer insight into attack vectors. Liu et al. showed the architecture of counter-based hardware Trojan horses to study the activation requirements and payload execution [15]. The benchmark circuits like the ISCAS85 has been widely applied in assessing the Trojan detection methodology because of its standardized format and refutability [16].

According to Bushnell and Agrawal, basic ideas of electronic testing and fault modeling are the theoretical basis of most logic-testing-based Trojan detection methods [17]. In more modern times, Yasin et al. brought IC testing further to the forefront of vulnerability, suggesting oracle-less attacks on IC camouflaging, and that trusted and secure approaches to testing methods are necessary [18].

It is evident in the literature that there cannot be a single detection method which can cater to all type of hardware Trojans. Although logic testing and side-channel analysis are the most popular, they cannot be effective against stealthy Trojan designs and process variations. This is the reason why hybrid and multi-layer security models are necessary, and the proposed dual-layer solution combines hardware-level optimization-based anomaly detection with software-level IP traffic monitoring and alerts.

PROPOSED METHOD

The offered solution is a two-layered Trojan detector and network anomaly observable framework that combines a self-optimized cryptographic hardware consciousness with a software-based IP traffic observation in real-time and automated signal. It is meant to identify any stealthy Trojan clients with the help of correlation of the abnormal hardware-initiated behavior with the network-level hints, which defeats the weaknesses of hardware-only detection methods.

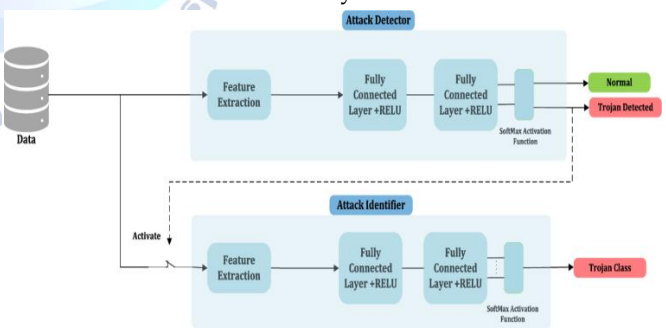


Fig1. Dual Layer Trojan detection and network anomaly proposed.

A. System initializing and designing.

The system operation commences with the initial stage of the system which is the system initiation stage during which all the necessary software, network interface, and configuration parameters are loaded. They import python-based libraries that handle packet capture, network scanning, data processing, visualization as well as network communication through email. Request rate limits, traffic volume limits as well as monitoring intervals are detected using the control panel interface.

This is done in order to achieve repeatable system behavior as well as tune it dynamically according to deployment needs.

B Network Discovery and Identification of devices.

After initializing the network scanning module, ARP scanning and ping sweeping takes place to determine all the active devices in the local connection. A unique profile containing IP address, MAC address, hostname, and vendor are added with each detected device. This step provides the baseline network map which is continually modified with the entry or exit of devices within the network. The proper discovery of the devices is essential in monitoring the behavior of traffic and linking suspicious activity with definite IP sources.

C. Packet Capture and Traffic Feature Extraction

Upon network discovery, the packet capture is started by the monitoring module in real-time. The packet handler intercepts and parses incoming and outgoing packets to obtain information on the header level including source and destination IP address, protocol type, size of the pack, and a timestamp. Each IP address has traffic characteristics in terms of request frequency, overall data volume and protocol usage patterns calculated. These features that are extracted represent the main input of the anomaly detecting engine.

D. Suspicious Activity Detection Mechanism

A suspicious activity detection component keeps analyzing extracted traffic characteristics and comparing them to the predefined thresholds. A strange behavior like heavy request rates in a short time interval, abrupt increase in data rate or excessive use of protocols is considered suspicious. The module will work as Attack Detector and will differentiate between normal and possibly malicious traffic. The decision mechanism of threshold allows a low computational overhead and is also capable of real-time detection.

E. Attack Identification and Classification

After a suspicious activity is observed, the system triggers Attack Identifier stage, which goes further to identify the flagged traffic patterns to establish the type and intensity of the attack. This level associations various indicators includes the frequency variations, volume variation, protocol discrepancy in order to detect the Trojan behavior. Anomalous IPs, sensing reason, and statistical parameters are summarized to the detected events in comparison table that are later analyzed.

F. Email Alerting and Incident Reporting Automated

System has built in automated email alert to be able to respond fast. When malaise activity is confirmed, an alert message of suspicious IP address, the reason of detection, and time are created and forwarded to the administrator. This real-time notification system provides a great time saving detection-to-response alert and allows timely responses to mitigate the threat which may be to block IP or isolate a system.

G. Data Visualization and Logging Data structures

Data structures Data structures are defined as the format which data is represented in a given system or program. The data visualization module shows real-time network traffic statistics in the chart, heat maps, and graphs, which allows an easy observation of the network activity. Also, every traffic information that is collected and every anomaly is recorded and saved in formatted data to be accessed later and analyzed via the offline data as well as in the case of audit and the future training of models. This logging in totality increases transparency of the system and allows forensic investigation.

H. Dismissal and Conclusion and Generation

Lastly, the system will produce an overviewed comparison table of anomalous IPs, traffic-statistics, and detection results and later end termination of monitoring activities. This summary gives a brief vision of the network security status at the time of monitoring and assists an analysis of the events after it occurred. The proposed system uses protocol dual-layers network anomaly and Trojan activity detection framework, which constantly monitors standard traffic at the packet level and integrates behavior indicators to report malicious actions.

Workflow:

After application initialization, it loads the requisite Python libraries, network interfaces and configuration parameters. A sidebar-based control panel (rendering the graphical user interface or GUI) is provided to enable the administration to set detection thresholds, enable monitoring modes, and have a view of live traffic statistics. After that, system activates network scanning module that performs ARP scanning and ping sweeping to detect connected devices and running IP addresses. Low-level sniffing mechanisms then initiate packet capture in which the incoming and outgoing packets are read and the relevant fields of the packet headers, the protocol and the source and destination IP address as

well as the volume are extracted. The packet handler module keeps real-time counters of the frequency of requests, volume of data and the volume of protocol usage which allows the fine tracking of traffic utilized by the individual IP address. Suspicious activity detection engine continuously carry out comparisons of parameters of observed traffic against predefined thresholds. Irrational request rates, irregular volume bursts, or some strange protocol transactions are noted as possible events caused by Trojan. Anomalies are detected and stored in comparison table to have them summarized statistically and analyzed in a forensic way. At the same time, email alerting module, sets automatic messages with the offending IP, reasons of detection and date which are immediately acquired by system administrator. Lastly, the data visualization module displays traffic graphs, heat maps and trends of usage on dashboard allowing a user to understand network behavior mostly intuitively and enabling quick decision making.

Proposed technique also successfully incorporates real time traffic analysis of the network, detecting anomalies, and automatic alerting under the same framework. The system allows the early detection of Trojan-related activity and the unauthorized access attempt by combining the packet-level monitoring and clever classification and visualization. This two-layered design improves the detection accuracy, scaling aspects and reaction efficiency hence is appropriate in the secure embedded systems and network related systems.

Python - Visual Studio Software Description:

The suggested system is created with Python and Visual Studio Code as the integrated development environment to organize and maintain the modules easily and debug. Real time monitoring and anomaly detection is applied by using Python libraries including packet-sniffing, networking and data analysis and visualization frameworks. Visual Studio Code offers a portable approach that enables one to have a smooth experience through visualization representation of the code and its deployment of the security monitoring application.

RESULTS AND DISCUSSION

This section contains the experimental findings following the implementation of suggested dual-layer Trojan detection framework, which combines AES-based anomaly detection optimization via optimized AES-based anomaly detection. Dashboard visualization, graphs of traffic analysis, data logging, as well as email alerts demonstrate the effectiveness of the system. A. Monitoring of Network and IP Detection Dashboard

A. \

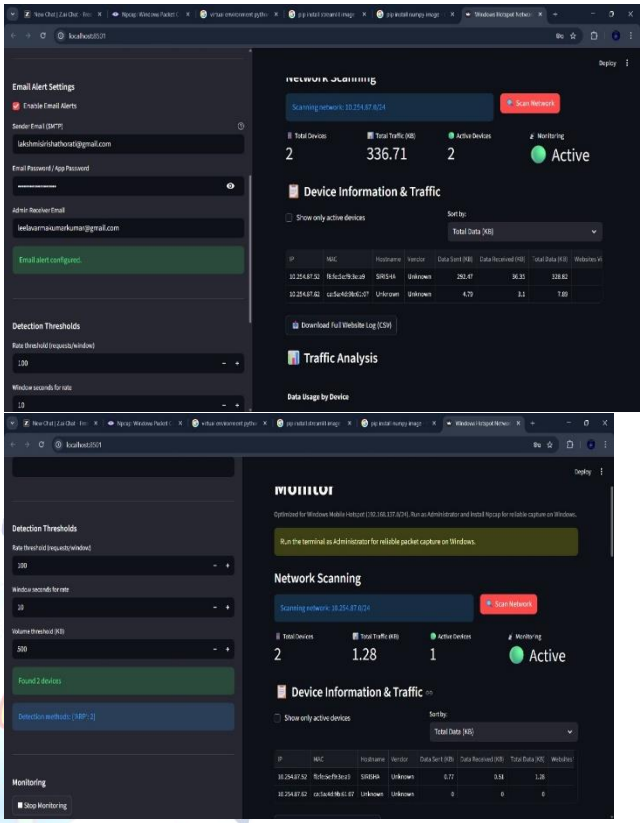


Fig 2. Connect Ip's On Dashboard

Fig.2 show the monitoring dashboard of a proposed system in real-time. Dashboard shows the connected IP devices amount, total network traffic, and the activity of the devices. The system scans the local network continuously, and identifies attached IP addresses and their relative traffic statistics.

The "Monitoring Active" status establishes that the detection module is working without failure. This live visibility allows intruders to predict suspicious behavior early enough and this is vital in establishing Trojan initiating activity, which requires based on network activity. The findings indicate that system is able to find the various devices and deliver live monitoring in the normal operating conditions.

B. Traffic Analysis and Graphical Representation

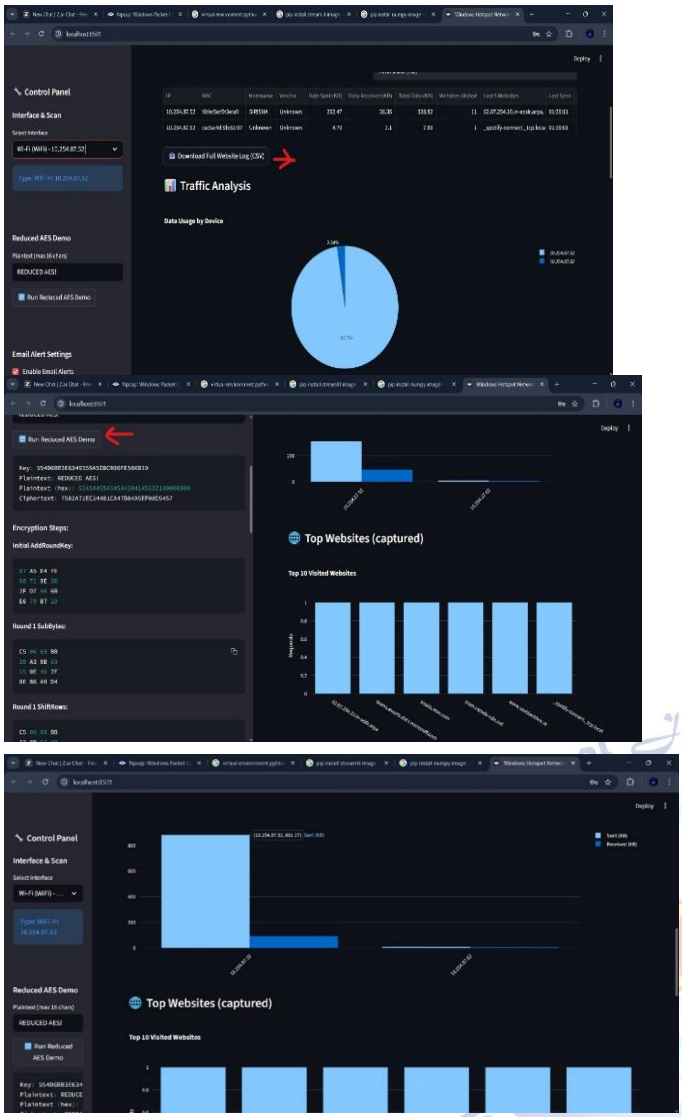


Fig3. Graph Readings

The graphical analyses of network traffic captured at the monitoring stage are provided in Fig. 3. These charts contain the bar charts and pie charts depicting data used by each device, data sent and received, and distribution of the traffic among connected IP addresses.

The graphical outputs are unambiguous as far as the changes in the traffic trends of devices are concerned. Traffic is under predetermined conditions in normal situations. But in the instance of an IP that has an abnormally high request rates or data transmission, the deviation can be seen in the graphs. It proves that the Attack Detector module works, and this solution is based on the characteristics of traffic to differentiate between the ordinary and suspicious behavior.

C. Data Logging and Storage in Dataset

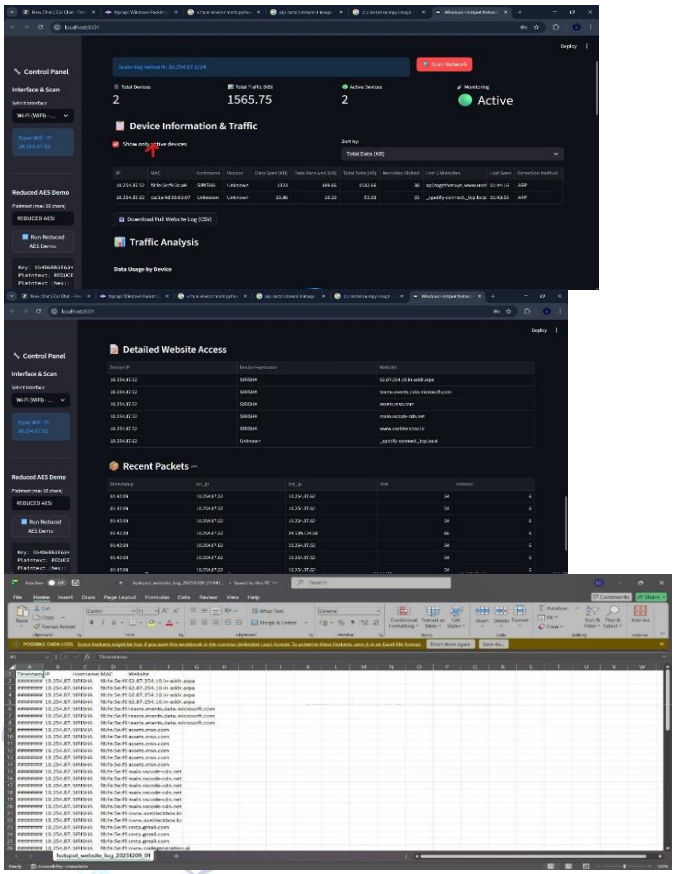


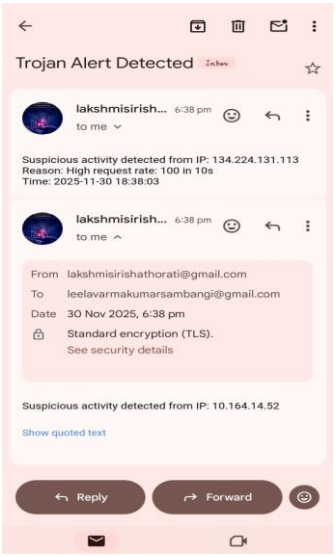
Fig4. Storing the Data in Data Sheet

Fig. 4 illustrates the storage of the stored network data in a form of structured spreadsheet. Parameters that are provided in each entry include: timestamp, IP address, MAC address, hostname, and accessed websites. This data repository has two significant applications offline analysis and forensic investigation.

Traffic information tracing

The power to record traffic provides the ability to trace unwanted activities and justify detection results. Furthermore, the stored information can be utilized in future work to train machine learning models in order to be better in detecting Trojan and anomalies.

D. Email Alert Notification System



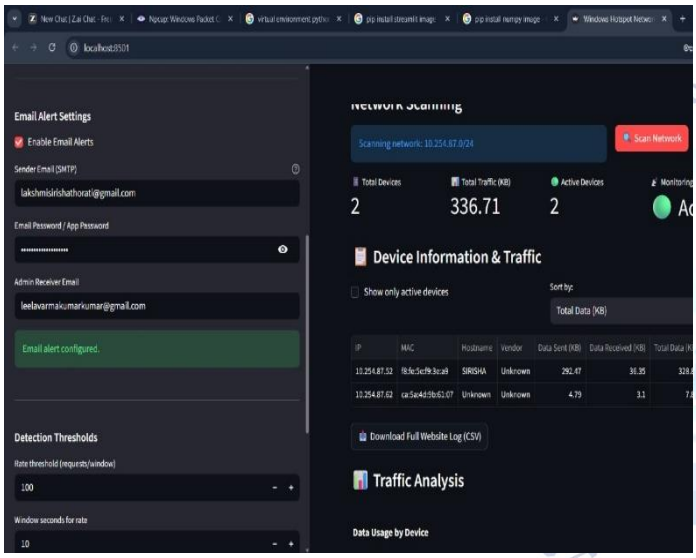


Fig5. (a) Email Output (b) Device Information Traffic

Fig.5 (a) and Fig. (b) Show the automated email alert system on the occurrence of a suspicious activity. On an IP goes above the set value on request rate or traffic volume, an alert system with the offending IP address, reason of detection, and time of detection is automatically generated.

This outcome justifies the usefulness of the Attack Identifier module that does not only verify the malicious activity but also initiates a real-time response. The automated notifications save a lot of time in terms of reaction and allow the administrators to undergo direct corrective action, including blocking the IP or isolating infected hardware devices.

The results of the experiment prove the idea of the dual-layer framework that integrates hardware-constrained protection concepts with the network-level-abnormal-detection methods. The situational awareness is given in real-time and the traffic analysis graphs are given to intuitively visualize the abnormal behavior.

In contrast to the conventional infrastructure used to assess Trojan horse hardware, which detect it based only on logic and/or side-channel evaluations, the suggested mechanism takes advantage of the network-activated behavioral markers thus being stronger against low-benefit Trojan horse ware with low hardware traces. The data logging mechanism contributes to transparency and auditability and the email alert mechanism allows quick incident response.

On the whole, these findings indicate that the suggested system can efficiently track the suspicious activities related to the Trojan behavior and issue the alerts in time enhancing the trustworthiness and reliability of the system with respect to security. This justifies the appropriateness of the framework presented to be used in secure embedded systems and cyber-physical settings.

CONCLUSION AND FUTURE SCOPE

The given paper introduced a dual-layer Trojan detection system which combines an Area Reduction AES architecture-based hardware-level anomaly detector and a software-based IP traffic monitoring and automatic alerts system. The proposed system can overcome the shortage of traditional logic testing methods and side-channel analysis methods, by making use of deviations upon resource utilization in cryptographic hardware, and correlation with abnormal network operation. Two stage model of detection Two stage model of detection: The two stage model, is composed of an Attack Detector and an Attack Identifier to improve the accuracy of the classification stage and to allow quick detection of malicious behaviour. The ability to monitor real-time IP and provide email alerts further assures the system as it is guaranteed that possible security breaches can be responded to in time to enhance the overall trust and resiliency of secure embedded and cyber-physical systems.

The work in the future will aim at building on the framework of the proposed work with advanced machine learning and deep learning features that detect threats adaptively in the context of dynamic attacks. The system can also be improved through the inclusion of

other side-channel parameters like electromagnetic emissions and temperature variations in order to enhance the detection strength to high-stealth Trojan. Also to be considered will be scalability to large-scale System-on-Chip (SoC) designs and testing on industrial benchmarks. Moreover, implementation of cloud based threats integration and automated mitigation systems could be introduced in the future, which allows reconfiguration of the system in real-time and proactive defensibility against the emergent threats to the hardware and network observable on the hardware or network layer.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Abbassi, I. H., Khalid, F., Rehman, S., Kamboh, A. M., Jantsch, A., Garg, S., & Shafique, M. (2019, March). Trojanzero: Switching activity-aware design of undetectable hardware trojans with zero power and area footprint. In 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 914-919). IEEE.

[2] K. Xiao, D. Forte, Y. Jin, R. Karri, and M. Tehranipoor, "Hardware Trojans: Lessons learned after one decade of research," ACM Transactions on Design Automation of Electronic Systems, vol. 22, no. 1, 2016. Trojan detection based on logical testing," Journal of Electronic Testing, vol. 33, no. 4, pp. 381–395, 2017.

[3] S. Bhasin and F. Regazzoni, "A survey on Hardware Trojan detection techniques," in Circuits and Systems. IEEE, 2015, pp. 2021–2024.

[4] S. Saha, R. S. Chakraborty, S. S. Nuthakki, D. Mukhopadhyay et al., "Improved test pattern generation for HT detection using genetic algorithm and boolean satisfiability," in Cryptographic Hardware and Embedded Systems, ser. LNCS, vol. 9293. Springer, 2015, pp. 577–596.

[5] S. Narasimhan, D. Du, R. S. Chakraborty, S. Paul, F. G. Wolff, C. A. Papachristou, K. Roy, and S. Bhunia, "Hardware Trojan detection by multiple-parameter side-channel analysis," IEEE Transactions on computers, vol. 62, no. 11, pp. 2183–2195, 2013.

[6] X. Zhang and M. Tehranipoor, "Detecting Hardware Trojans in ThirdParty Digital IP Cores," in Hardware-Oriented Security and Trust (HOST). IEEE, 2011, pp. 67–70.

[7] A. Bazzazi, M. T. M. Shalmani, and A. M. A. Hemmatyar, "Hardware Trojan detection based on logical testing," Journal of Electronic Testing, vol. 33, no. 4, pp. 381–395, 2017.

[8] V. Govindan and R. S. Chakraborty, "Logic testing for Hardware Trojan detection," in The Hardware Trojan War. Springer, 2018, pp. 149–182.

[9] . S. Chakraborty, F. G. Wolff, S. Paul, C. A. Papachristou, and S. Bhunia, "MERO: A statistical approach for Hardware Trojan detection." in Cryptographic Hardware and Embedded Systems (CHES), ser. LNCS, vol. 5747. Springer, 2009, pp. 396–410.

[10] G. Di Natale and Dupuis, "Is side-channel analysis really reliable for detecting Hardware Trojans?" in Design of Circuits and Integrated Systems, (DCIS), 2012, pp. 238–242.

[11] R. Rad, J. Plusquellic, and M. Tehranipoor, "A sensitivity analysis of power signal methods for detecting Hardware Trojans under real process and environmental conditions," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 18, no. 12, pp. 1735–1744, 2010.

[12] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware Trojan horse detection using gate-level characterization," in Design Automation Conference (DAC). IEEE, 2009, pp. 688–693.

[13] X. Chen, L. Wang, Y. Wang, Y. Liu, and H. Yang, "A general framework for hardware trojan detection in digital circuits by statistical learning algorithms," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 36, no. 10, pp. 1633–1646, 2017.

[14] S. K. Haider, C. Jin, M. Ahmad, D. Shila, O. Khan, and M. van Dijk, "Advancing the state-of-the-art in Hardware Trojans detection," IEEE Transactions on Dependable and Secure Computing, 2017.

[15] H. Liu, H. Luo, and L. Wang, "Design of Hardware Trojan Horse Based on Counter," in Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2011. IEEE, 2011, pp. 1007–1009.

[16] "ISCAS85:," http://web.eecs.umich.edu/ jhayes/iscas.restore/, 2018.

[17] M. Bushnell and V. Agrawal, Essentials of electronic testing for digital, memory and mixed-signal VLSI circuits. Springer Science & Business Media, 2004, vol. 17.

[18] M. Yasin, O. Sinanoglu, and J. Rajendran, "Testing the trustworthiness of ic testing: An oracle-less attack on ic camouflaging," IEEE Transactions on Information Forensics and Security, vol. 12, pp. 2668–2682, 2017.