ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Investigation of Firmware Securing IoT Devices at the Chip Level Using AI and ML Approaches: A Concise Systematic Literature Review

Rajat Suvra Das

Senior Director, Business Development, L&T Technology Services, USA

ABSTRACT

System-on-Chip (SoC) designs are becoming increasingly intricate as they integrate various components and functionalities onto a single chip. This intricacy brings forth new vulnerabilities and attack surfaces, presenting a challenging task to ensure robust cybersecurity. Although previous studies have explored different AI approaches, there is a need to delve into the complexities of modern SoCs and propose practical methods to secure these systems, thereby aiding researchers in mitigating potential threats. The primary objective of this paper is to uncover the opportunities that emerge from utilizing AI techniques in SoC designs to fortify cybersecurity defenses. Subsequently, the study aims to deliberate on the complexities involved in integrating AI with SoC and provide appropriate recommendations to address these intricacies. This review paper will identify and discuss the technical, architectural, and implementation challenges faced by researchers and practitioners when incorporating AI into SoC designs for cybersecurity purposes. Moreover, it will suggest with potential solutions and strategies to effectively tackle these challenges. Furthermore, it aims to aid future researchers by offering potential research directions to enhance security in AI-SoC through innovative solutions. By identifying gaps in current literature and highlighting areas that require further exploration, this paper will guide future researchers in developing advanced and secure AI-SoC systems for cybersecurity applications. Overall, this review paper will contribute to the existing body of knowledge by providing a comprehensive analysis of the impact that integrating AI and SoC has on cybersecurity and foster advancements in AI-SoC systems that effectively enhance cybersecurity measures.

***Corresponding author**

Rajat Suvra Das, Senior Director, Business Development, L&T Technology Services, USA.

Received: December 08, 2023; **Accepted:** December 14, 2023; **Published:** December 21, 2023

Keywords: Internet of Things, Firmware, Chip level security, Challenges, Semi-Conductors

Introduction

Firmware is a form of microcode embedded into hardware devices for helping to operate effectively [1]. It is essentially defined as a category of software permanently embedded into the device ROM (Read Only Memory), which provides instruction on how the device is supposed to operate and minimizes the hardware level security vulnerabilities. Usually, firmware is the first part that runs when a device is powered on. It sends instructions for execution to the device processor. In simple devices, the firmware works continuously; however, in more complex device, multiple firmware is used to accomplish daunting and challenging tasks. Thus, three types of firmware are used [2].

Low-level, high-level, and subsystem are three types of firmware parts; low-level firmware cannot be modified or altered as they are assessed as integral hardware; however, high-level firmware often has a higher instruction complexity than low-level firmware [3]. Eventually, subsystems are parts of more extensive systems that can work independently and possess power, like high-level firmware in terms of operation. Typically, Firmware updates and enhances the functionality and features of the devices. Due to the functionality of firmware, it can be used in IoT devices. However, security is considered one of the major drawbacks of IoT devices; some possible challenges include lack of reliable IoT standards, use of third-party components, insecure network connection, poor device patching and management, and many more. Hence, it is important to identify the vulnerabilities as quickly as possible [4,5].

Moreover, firmware security should also be considered to deliver the desired outcome to the end-users since IoT devices can be vulnerable to hacks and loose ends in firmware [6]. As distinct components are embedded in the firmware, the kernel can be manipulated only if boot loader access is accessible. Therefore, securing firmware starts with examining it to find the loopholes.

Eventually, IoT device firmware is created to let the users control the devices as per the desired outcome. As IoT firmware level security is extremely important, it is predominant to execute IoT firmware level security systems for protecting the systems against cyber-attacks; by doing so, it also enables robust IoT security management and monitoring in the long run [7]. Another significant aspect of IoT devices is securing the devices at the chip level. Securing IoT devices at the chip level is extremely imperative for guaranteeing robust and comprehensive security. Thus, implementing security measures directly at the chip level can help create a strong foundation for protecting IoT devices

from different threats [8]. Securing IoT devices at the chip level involves incorporating security features directly into the hardware [9]. Further, chip-level security facilitates the implementation of robust cryptographic algorithms and protocols. This helps in securing the communication between the IoT devices and other components.

In addition to these factors, chip-level security enables the implementation of a strong encryption mechanism, which ensures sensitive data transmitted or stored in the device remains confidential and protected from unauthorized access [10]. By doing so, it aids in preventing data breaches and safeguarding user privacy. Owing to these factors, the present SLR paper focuses on securing the firmware of IoT devices at the chip level. Thus, the objectives of the paper include,

- To conduct survey methodology for scrutinizing the appropriate papers by employing different criteria like inclusion criteria and exclusion criteria.
- To deliberate the critical role of semi-conductor components in IoT security.
- To discuss the conventional and AI methods for firmware securing IoT devices at the chip level.
- To summarize the challenges of the prevailing works and focus on delivering future recommendations.

Paper Organization

The paper is organized as follows. Section II deals with survey methodology, Section III focuses on the critical role of semi-conductors, Section IV emphasizes implications of chip-level security in IoT devices, Section V deals with conventional methods applied for chip-level security for IoT devices, Section VI focuses on AI and ML approaches for chip level security for IoT devices, Section VII emphasizes on challenges and future recommendation to overcome these limitations and conclusion of the present SLR is depicted in Section VII.

Survey Methodology

The corresponding section focuses on the techniques for obtaining relevant papers using different inclusion and exclusion criteria, which will be focused on in the upcoming section.

The Process Incorporated in Shortlisting Papers for SLR

This section defines the sequential process implemented for determining the appropriate papers that should be reviewed in this SLR. The four common sequential steps of this selection of relevant papers are below in Figure 1.

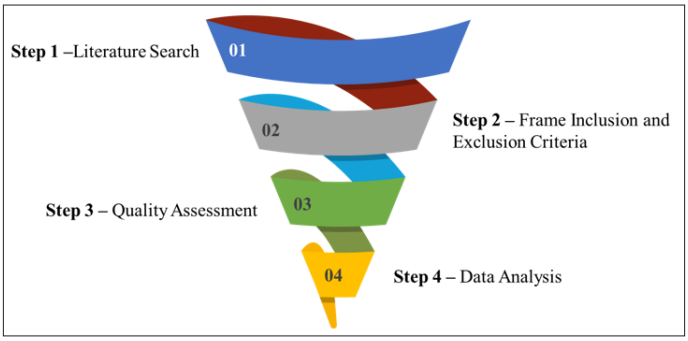

Figure 1: Survey Approaches

Step 1: Literature Search

The step includes defining the search terms to determine data sources and identify the data collection process.

Step 2: Frame Inclusion Criteria and Exclusion Criteria

In this step of SLR, specific criteria were defined for guiding the extraction process of the most appropriate relevant research or studies.

Step 3: Quality Assessment

In this phase, every article or the extracted journal papers was reviewed based on three criteria categories in quality evaluations. The section was elaborated in the following upcoming section.

Step 4: Data Analysis

Once the selected researchers were reviewed, the appropriate data were extracted and recorded in the chapter.

An in-depth analysis is depicted in the subsequent section.

Criteria for Searching the Literature

The well-refined databases are applied to pursuit pertinent papers using the related keywords. The electronic scientific database and data sources used to select the papers are below.

- Google Scholar
- IJARET
- IEEE
- Research Gate Journals
- ACM
- Springer
- MDPI
- Science Direct
- Other Databases

As the journals above offer more thorough coverage of the chosen topic, the databases are used in this SLR.

Search Terms Used

Numerous pertinent search terms are incessantly used to get appropriate papers. Different keywords like “Firmware," "Firmware in IoT security," "Chip level security in IoT devices," "AI methods for Firmware detection," “Challenges and Future work," “Significance of chip-level security," and other keywords are used for searching the term.

The sources chosen included literature surveys, research papers, case studies, review papers, proceedings, or empirical studies.

Required Information from Selected Papers

The required information was taken from the abstract or the whole document.

The Publication Period of Records

Papers after 2017 are considered in the present SLR

Inclusion Criteria and Exclusion Criteria

Different inclusion and exclusion criteria are used to choose the right papers, articles, etc.

Inclusion Criteria

- The paper presents research papers, a literature review, and a review paper with a defined abstract, methodology, title, and findings.
- The entire research work must be related to the study area.

Exclusion Criteria

The papers can be excluded if the articles, papers, or reviews if the records follow the below condition

- Duplication of findings is omitted.
- Irrelevant abstract and title.

- The conventional literature reviews were excluded, which have undefined research questions, undefined search processes, and nil well-distinct data extraction phases.
- If the articles or records were not written in the English language.

Quality Evaluation

- **QE1:** Does the paper offer clear implications with justifiable outcomes and their conclusions?
- **QE2:** Does the paper cover relevant research work and explore research topics comprehensively?
- **QE3:** Do the articles, papers, or reviews provide future directions?

Shortlisted Refined Papers for this SLR and Categorize them into Broad Areas

The paper was shortlisted based on the research question, objective, topic, and scope. The papers are selected based on firmware securing IoT devices at the chip level and to find the limitations of the selected studies in the applied area.

The selected papers in every area were briefed in the upcoming section, with their objectives, conclusion, or the inferences and limitations of the study, and the concise diagram is depicted in Figure 2.

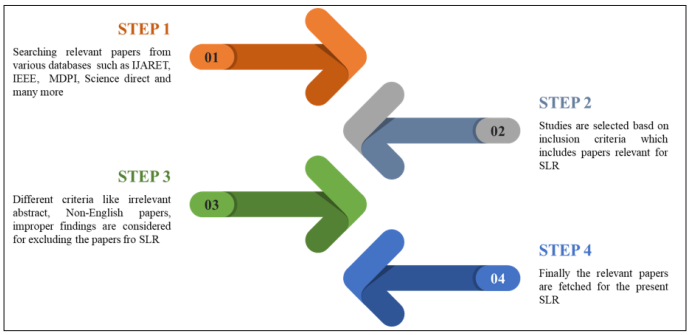

Figure 2: Summary of Survey Methods

Figure 2 shows the steps in fetching the relevant content and appropriate papers required for reviewing the existing works. Therefore, by implementing these steps, the present SLR has obtained 23 relevant papers, and a review of the prevailing works will be explored in the upcoming section.

Critical Role of Semi-Conductor Components in IoT Security

Semi-conductors play a critical role in IoT security. These components are important for enabling secure communication, encryption, and authentication in IoT devices. They provide the necessary hardware support for implementing robust security measures, which include secure booting, secure storage, and secured key management. Moreover, semiconductor components enable secured communication protocols, including TLS (Transport Layer Security), which encrypts data transmission between connected devices and IoT devices. These encryption devices also aid in safeguarding sensitive information from manipulation or intervention. Table 1 shows the role of semiconductors in IoT security.

Table 1: Role of Semi-Conductor in IoT Security

Function	Description
Secure Boot and Firmware Integrity	Semiconductor components aid in establishing a secure boot process, which facilitates ensuring trusted and verified firmware loaded on IoT devices.
Hardware-Based Security	Semiconductor components offer hardware-based security features that are more likely to resist software-based attacks.
Secure Verification	Semi-conductor-based components enable secured authentication mechanisms like cryptographic keys and certificates, which help verify IoT device identity.
Encryption and Protection of Data	Semiconductor components usually support encryption algorithms that protect the sensitive data transmitted between IoT devices and connected devices.
Detection of Tamper and Response	Certain semiconductors can aid in the detection of tamper. This tamper detection helps in detecting physical attacks on the devices.

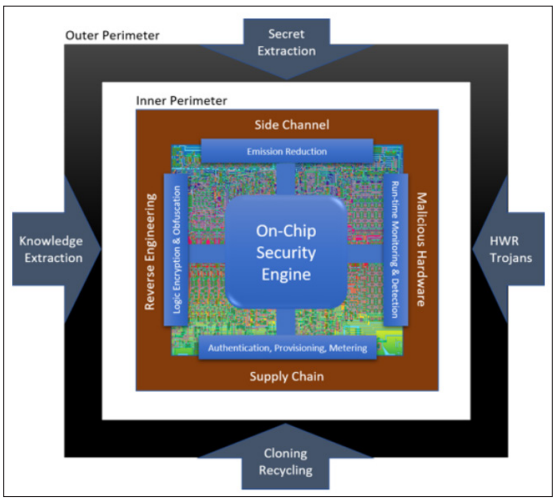

Figure 3: Secure Chip Architecture [11]

Figure 3 depicts the on-chip security engine. Plummeting the risk of probable hardware breaches requires a rock-solid understanding of chip architecture, which includes everything from segregating and prioritizing data movements to storing data and other aspects. However, accomplishing all these aspects can be complex and challenging, nevertheless, building a chip by considering all these factors can make the hackers difficult to hack. In addition, accomplishing these tasks requires a lot of effort and money. Further, not all components are innately protected and not always perfect, which ones have been designed with security in mind as many of these tailored accelerators and IP Blocks are established as black boxes. Besides, another bigger challenge includes the longevity of the hardware design, as security needs to be end-to-end. This can be reprogrammed to deal with different threats, which is particularly helpful in dealing with threats to chips with extended lifetimes.

Implications of Chip-Level Security in IoT devices

As with any embedded system, IoT design faces persistent threats, and since hacker uses different attacks, developers are in dire need of closing security holes. In deployed devices, the constant requirement to update IoT firmware adds impending weakness in security. For instance, even modest firmware validation checks may result in software exploitation. Further, in most cases, developers attempting to query some exterior resource for validation may hook attempts to switch firmware with code that has been hacked. Thus, some of the major significance of chip-level security for IoT devices include,

- **Long-Term Resilience:** Chip-level security can offer long-term pliability against different evolving threats.
- **Secure Communication:** Chip-level security helps secure the communication between IoT devices and other systems.
- **Enhanced Protection:** Instigating security measures at the chip level provides a strong foundation for protecting IoT devices against probable attacks and other vulnerabilities.
- **Protection of Sensitive Data:** IoT devices often handle sensitive data, which includes personal information or other crucial data.
- **Trustworthiness and Compliance:** Chip-level security plays a massive role in establishing trust in IoT devices for end users and regulatory bodies.

Thus, these factors are considered some of the major significances that emphasize IoT devices' security level. The subsequent section deals with different traditional techniques used for firmware security in IoT devices at the chip level.

Conventional Techniques for Firmware Security in IoT Devices at Chip Level

Identifying vulnerability is one of the crucial aspects of security, as this helps ensure the model's security. Therefore, static and dynamic analysis is used in the subsequent section for firmware security in IoT devices at the chip level. Thus, IoTFUZZER has been used for finding memory corruption vulnerabilities in firmware [12]. From the experimental outcome, it was identified that, out of 17 IoT devices, 15 devices were corrupted due to vulnerabilities. However, the IoTFUZZER model has focused on providing only the input data that triggers the vulnerability, not the precise location of the vulnerability in the firmware.

Similarly, a Firm Fuzz mechanism has been used for dynamically investigating the vulnerability of Linux-based IoT devices. To detect the vulnerability, Firmware fuzzing gas been used. Firm Fuzz has the capability to discover 7 strange vulnerabilities in 6 different devices. The Firmup approach has been used to identify the techniques, vulnerabilities, and exposures in stripped firmware images [13]. It established a correspondence between the set of measures in a given binary and a target binary. Moreover, the implemented Firmup model has expansively assessed millions of procedures and detected around 373 vulnerabilities.

The emergence of IoT networks has increased the need for higher security levels [14,15]. Further, the consumption of energy, the cost of the device, and extensive cryptographic algorithms also serve as an additional challenge for resource-constrained devices. Thus, to overcome these challenges, semiconductor vendors have used dedicated hardware called secure elements, which provide hardware-accelerated support for cryptographic operations and aid in tampering with the memory for securing the storage of cryptographically complex material [16]. The supporting secure elements include A71CH from NXP and ATECC608A from Microchip, and the standalone chip comprises OPTIGA Trust X from Infineon and TO136 from trusted objects. The design of the 4 secure elements is depicted in Figure 4.

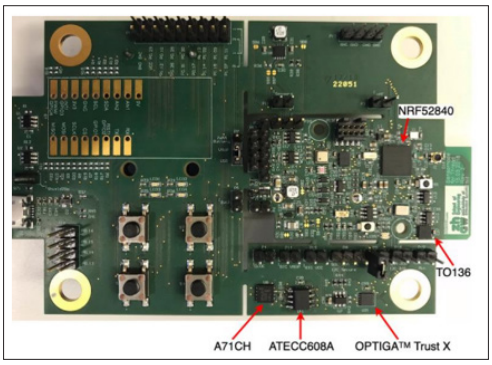

Figure 4: Chip with 4 Different Secure Elements [16]

The results of the performed evaluation have stated that there have been major differences regarding the execution time and the consumption of energy between these 4 selected secured elements. Though these secure elements aid in different applications, the evaluation also emphasizes the difficulty of integrating secured elements into an application, as IoT devices require immense effort. In the IoT edge node, the microcontroller/ SoC (System of Chip) is considered an important component, as the SoC utilized in the sensitive application comprises of TEE (Trusted Execution Environment). However, TEEs are not so effective enough to address all security issues for security. Therefore, PUF (Physical Unclonable Function) and cryptographic modules have been emphasized in the work as they may detect edge nodes in IoT, help in mitigating fabrication, and authenticate the devices while updating the firmware in IoT edge nodes.

Globalization of semiconductor manufacturing and other related activities have eventually led to different security issues such as cloning, IP address infringement, counterfeiting, and many more. However, this counterfeiting not only affects the reputation and the business of the semiconductor vendor but also the dependability of different applications. Thus, SSTF (Secure Split Test with Functional Testing Capability) is used for mitigating the counterfeits from untrusted fraud. However, SSTF is only suitable for low-end devices, to overcome these limitations, PUF is combined with SSTF to help out chip makers effectively [17].

AI and ML Techniques Firmware Security in IoT devices at the Chip Level

The security of chips is considered one of the crucial issues in IoT security. In recent times, as the amount of data processed proliferates intensively, the equipment of each layer requires a more complex design to improve the processing power. Thus, the incorporation of chips is getting higher and higher; however, ensuring the security of chips at a large level is extremely challenging and demanding. Thus, the study has focused on employing an ML-based hardware–Trojan detection approach [18].

Firmware detection focuses on employing different tactics using ML methods. Thus, it is important to confirm the vulnerability of devices. Correspondingly, hybrid methodology has employed a double security mechanism for the firmware of IoT devices [19,20]. Here, a secure boot greatly elevates the firmware by employing cryptographic and ML methods. The technique utilized is the ECC-LSTM (Elliptic Curve Cryptography – Long Short

Term Memory) method, where the accuracy attained by the model has been 98.66%.

Mostly, encryption chips or cryptographic code processors in the hardware layer of IoT devices are often used for preserving hardware security and RTOS (Real Time Operating System). Likewise, the hardware layer is critical for IoT security [21]. Also, it helps in ensuring security measures, secure boot load, and help in firmware updates, which are authenticated by digital]signatures. Thus, Figure 5 shows the implementation of ML and DL approaches regarding sufficient and representative data, ML and DL construction, and, eventually, the model deployment.

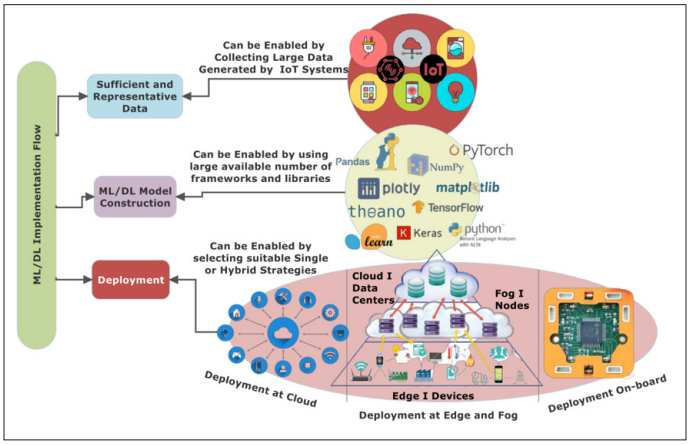

Figure 5: Implementation of IoT Devices with Deployment on Board [21]

The SoC design comprises various IP (Intellectual Property) cores that communicate using the NoC framework (Network on Chip). However, the designers of SoC exceedingly depend on global SC (Supply Chain) for attaining 3rd party IPs. Moreover, NoC-based SoCs are very much exploited for attacks and have resulted in a plethora of attacks. Thus, the ML-based XGBoost model has been used for identifying security threats at the chip level [22]. From the experimental outcome, it was identified that a better outcome has been attained for detecting the attacks.

Challenges and Future Recommendations

The subsequent section depicts challenges and future recommendations for chip-level security in IoT devices.

- **Limited Resources:** IoT devices often have constrained resources, including memory, power, and energy, which make it daunting to implement robust security measures at the chip level.
- **Cost Constraints:** IoT devices are considered to be generated at a large scale, and the cost consideration may restrict the inclusion of progressive security features at the chip level, which leaves them more vulnerable to attacks.
- **Firmware Updates:** IoT devices do not possess forthright mechanisms for firmware updates, thereby making it challenging and perplexing to patch security vulnerabilities or address emerging threats at the chip level.

Thus, to overcome these limitations, different recommendations can be incorporated in the future for obtaining better performance, which includes

Securing Firmware Updates

Developing a secured mechanism for updating firmware on IoT devices is considered one of the essential aspects that need to be emphasized in the future, as this will be very helpful for securing communication channels and bootloaders from unwanted and unauthorized firmware alterations.

Confidentiality Protection

Addressing concerns related to IoT devices is tremendously crucial. Thus, future work involves employing privacy-enhancing technologies like differential privacy, secure data-sharing protocols, data anonymization, and many more.

Authentication and Access Control

Strengthening the authentication mechanism and access control protocols ensures that only authorized entities can access and interact with IoT devices. Therefore, exploring different advanced authentication techniques for upholding effective privacy mechanisms is crucial.

Apart from these future recommendations, there are other future works that can be emphasized for preserving security at the chip level in IoT devices.

Conclusion

Firmware is one of the few components that needs to be secured as it plays a crucial role in enabling the system's performance, functionality, and security. Thus, the present SLR focuses on reviewing different works that stress the security of IoT devices at the chip level. In order to accomplish this, different inclusion and exclusion criteria are used for obtaining the relevant papers; from the obtained work, it was identified that around 23 papers were obtained to be relevant. SLR covered the implications of securing the chips of IoT devices, conventional methods, AI techniques for detecting the attacks faced by firmware, and ways to secure the IoT devices at the chip level. Despite the existing studies having delivered considerable performance, a few challenges, such as the updation of firmware and constrained resources, can be overcome in the future by employing effective measures. Besides, the present SLR can also help technical enthusiasts uncover the importance of the chip-level security of IoT devices due to the rise of IoT devices in the coming time [23].

References

1. Leah Hoffmann (2023) Achievement in Microarchitecture. Communications of the ACM 67: 50.
2. Mohammed Aziz Al Kabir,Wael Elmedany, Saeed Sharif Mhd (2023) Securing IoT devices against emerging security threats: challenges and mitigation techniques. Journal of Cyber Security Technology 7: 199-223.
3. Sheptunov SA (2023) Firmware Intellectual System Application in Quality Management. 2023 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS) 34-39.
4. Rekha S, Thirupathi L, Renikunta S, Gangula RJMT (2023) Study of security issues and solutions in Internet of Things (IoT). Materials Today: Proceedings 80: 3554-3559.
5. Amali C, Guru K, Sridevi D (2020) IoT Based Smart Logistics Management System using GPS and GSM. IJARET 11: 3035-3041.
6. Nadir I, Mahmood H, Asadullah G (2022) A taxonomy of IoT firmware security and principal firmware analysis techniques. International Journal of Critical Infrastructure Protection 38: 100552.
7. Katbi A, Hammad M, Ksantini R (2023) A Survey on IOT Firmware Security. University of Bahrain Scientific Journals

14: 190-199.

8. Rizvi S, Pipetti R, McIntyre N, Todd J, Williams I (2020) Threat model for securing internet of things (IoT) network at device-level. Internet of Things 11: 100240.
9. Farahmandi F, Huang Y, Mishra P (2020) System-on-chip security. Springer https://www.springerprofessional.de/en/system-on-chip-security-vulnerabilities/17421832.
10. Klimushin P, Solianyk T, Kolisnyk T, Mozhaiv O (2021) Potential application of hardware protected symmetric authentication microcircuits to ensure the security of internet of things. Advanced Information Systems 5: 103-111.
11. Sperling E (2021) Why It's So Difficult - And Costly - To Secure Chips. SemiConductor Engineering https://semiengineering.com/why-its-so-difficult-and-costly-to-secure-chips/.
12. Salehi M, Degani L, Roveri M, Hughes D, Crispo B (2022) Discovery and Identification of Memory Corruption Vulnerabilities on Bare-metal Embedded Devices. IEEE Transactions on Dependable and Secure Computing 20: 1124-1138.
13. Rocha TA, Martins AT, Ferreira F (2020) Synthesis of a DNF formula from a sample of strings using Ehrenfeucht–Fraïssé games. Theoretical Computer Science 805: 109-126.
14. Jurcut AD, Ranaweera P, Xu L (2020) Introduction to IoT security. Tech DOCS 27-64.
15. Rayan A, Taloba AI, El-Aziz A, Rasha M, Abozeid A (2020) IoT enabled secured fog based cloud server management using task prioritization strategies. International Journal of Advanced Research in Engineering and Technology 11: 697-708.
16. Schläpfer T, Rüst A (2019) Security on IoT Devices with Secure Elements. Embedded World Conference 2019 - Proceedings https://digitalcollection.zhaw.ch/handle/11475/16297.
17. Kumar KS, Rao GH, Sahoo S, Mahapatra K (2017) Secure split test techniques to prevent IC piracy for IoT devices. Integration 58: 390-400.
18. Dong C, Chen J, Guo W, Zou J (2019) A machine-learning-based hardware-Trojan detection approach for chips in the Internet of Things. International Journal of Distributed Sensor Networks 15: 1550147719888098.
19. Punidha A, Arul E, Yuvarani E (2023) Firmware Attack Detection Using Logistic Regression (FAD-LR). Atlantis Press 37-41.
20. Devi RA, Arunachalam A, Rajakumar PJD (2020) Development of Advanced IoT Devices using ECC-LSTM for an Enhanced Device Security. International Journal of Advanced Science and Technology 29: 5074-5087.
21. Sharma P, Jain S, Gupta S, Chamola V (2021) Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. Ad Hoc Networks 123: 102685.
22. Sudusinghe C, Charles S, Mishra P (2021) Network-on-chip attack detection using machine learning. Network-on-Chip Security and Privacy: Springer 253-275.
23. Kumar SK, Sahoo S, Mahapatra A, Swain AK, Mahapatra K (2017) Security Enhancements to System on Chip Devices for IoT Perception Layer. 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS) https://ieeexplore.ieee.org/document/8293922.

Copyright: ©2023 Rajat Suvra Das. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.