[1]Paidimalla Naga Raju,
2Raghu Kalyana,
3D.N.V.S.Vijaya Lakshmi,
4V.Rambabu

Low-Power Security Solutions for IOT Applications

JES Journal of Electrical Systems

Abstract:

The Internet of Things (IoT) is a technical advancement that has transformed civilization. The Internet of Things will irrevocably transform our use of basic objects into intelligent, fully functional devices. IoT devices may execute and automate routine domestic and occupational operations using basic sensors. Despite the advantages of these gadgets, they remain susceptible to infringements, including privacy concerns and security breaches. This study seeks to elucidate the vulnerabilities of IoT devices and the contemporary dangers they face. Additionally, the technologies used in the IoT are analyzed, along with the various communication layers of the IoT and their operations. The results indicate that IoT devices are susceptible to several software and hardware vulnerabilities, as well as the associated problems of IoT. Proposed solutions to these difficulties include the implementation of anomaly-based intrusion detection systems, which are essential elements of network security. Employing machine learning (ML) for the identification of possible assaults is advisable. Numerous suggested anomaly-based detection systems use various machine learning algorithms and methodologies. Nonetheless, there exists no standardized baseline for comparing them regarding power usage. A benchmark is provided to assess both accuracy and power usage for evaluating each algorithm's implementation.

Keywords—Efficient; IoT; Systems on a Chip (SoC); ML; Network

INTRODUCTION

The world is seeing a swift and exhilarating shift due to the extensive accessibility of systems on a chip (SoCs), as seen in Fig. 1. SoCs enable the development of very complex and compact computer models capable of network connectivity.

When a System on Chip (SoC) connects to the Internet, it becomes part of the Internet of Things, establishing a crucial basis for several services. Our daily existence depends on their efficacy and the quality of their performance. For instance, industrial uses. Conventional security methods are often more costly for IoT regarding energy consumption and administrative expenses. Most security frameworks are often centralized in response to a danger. Consequently, they are unsuitable for devices inside a dispersed network due to challenges related to scale, heightened traffic, and the presence of a single point of failure [2]. Gathering data from all facets of the industrial life cycle may substantially enhance performance, enabling a corporation to accumulate more data and oversee its industrial processes.

Furthermore, several additional devices may be connected to the network. Such systems often allocate the majority of their resources and computational capacity to the application's primary features; hence, maintaining safety and

[1] [1,2,3,4]International School of Technology and Sciences for Women, A.P , India.

privacy at a reduced cost will be very challenging. The main distinction between elliptic curve cryptography (ECC) and Rivest Shamir Adleman (RSA) is in the key size relative to cryptographic strength. Elliptic Curve Cryptography (ECC) may achieve much reduced key sizes while maintaining equivalent cryptographic strength to a Rivest-Shamir-Adleman (RSA) scheme. A 256-bit ECC key is equivalent to a 3072-bit RSA key. The escalating danger has necessitated the formulation of novel ways to identify and obstruct IoT botnet attack traffic. Recent studies have shown the potential of machine learning (ML) in detecting harmful Internet traffic [4]. Nonetheless, machine learning models primarily focused on IoT application networks or IoT attack vectors have seen little success. Fortunately, IoT traffic often differs from that of other Internet-connected devices (e.g., laptops and cellphones) [5].

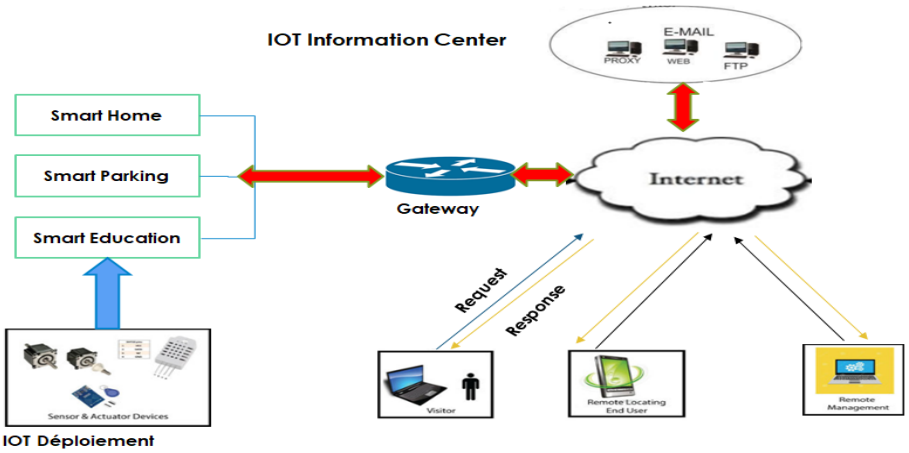

Fig. 1. Overview of IoT components.

The remainder of this work is structured appropriately. Initially, the IoT layers will be delineated with the various wireless network technology possibilities and their respective features. The prevalent assaults on IoT devices and the fundamental design issues associated with them will be addressed. A review of current pertinent literature will be presented thereafter. Subsequently, we will provide an overview of the UNSW-NB15 dataset. Anomaly-based intrusion detection methods will be shown using six classifiers. The proposed solution will provide the approach for assessing the performance of Intrusion Detection Systems (IDS). The studied findings will be shown both with and without the proposed solution. In conclusion, we shall encapsulate our findings and outline prospective endeavors.

Literature Review

A literature survey of contemporary studies on security in resource-constrained devices, such as IoT devices. These gadgets are among the most economical alternatives for several daily uses. The number of devices linked to the Internet is steadily increasing. The International Data Corporation's newest prediction predicts 41.6 billion linked IoT devices would generate 79.4 zettabytes of data by 2025.

A. Relevant Literature

Sicari et al. [22] The authors examine secrecy, authentication, data security concerns, network security, intrusion detection systems, and the persistent absence of communication standards. Effective implementations must be devised and executed, irrespective of the technology used, to provide security, access control, user and object privacy, and device performance. Adherence to certain rules about security and data protection. Notwithstanding several endeavors in this domain, certain hurdles and research issues persist. The author asserts that there is an

absence of systems and a cohesive vision to guarantee the security of the Internet of Things. The author then analyzes multinational programs in this domain, noting that these initiatives often seek to develop and execute particular applications of the Internet of Things. The paper also addresses the need of using IoT technologies and communications inside secure middleware that can satisfy certain security requirements. Hongchun et al. [23] suggested a knowledge-based intrusion detection system to identify various forms of assaults across diverse network architectures. The objective was to develop an autonomous detection model reliant on the architecture of the WSN network. The proposed mechanism was predicated on the observation that various sorts of assaults may have distinct density shapes. The authors gathered network traffic and used it as a characteristic of random network activity inside the feature space. The density form serves as an indicator of both normal and aberrant network functioning. Simulation outcomes from assaults, like sinkholes, floods, or DoS, demonstrate that the technique exhibited suitable detection accuracy and substantial compliance with the network architecture. Stergiou et al. [24] Conduct a survey on the Internet of Things (IoT) in conjunction with cloud computing, focusing on the security challenges inherent to both technologies. This survey will analyze their integration, highlighting common characteristics and exploring the benefits derived from their convergence. They illustrate how cloud computing might enhance the security challenges associated with IoT integration. The theoretical application architecture and the integration of IoT and Cloud Computing, along with their security advantages, are further examined using the two used encryption algorithms: AES and RSA.

Doshi et al. [25] High precision DDoS assaults in IoT traffic may be discovered using various machine learning methods, including neural networks, by analyzing IoT network activity to detect attack features. The findings indicate that primary gateways or other key network nodes would autonomously categorize locally sourced IoT DDoS attack origins using cost-effective machine learning techniques and a standalone flow-based traffic data protocol. Denial of Service (DoS) detection may effectively distinguish between normal and DoS attack traffic using packet-level machine learning for Internet of Things (IoT) consumer devices. A limited number of attributes was used to minimize computational overhead, which is crucial for the real-time identification and deployment of the middlebox. Their feature selection was predicated on the notion that network traffic patterns for IoT application clients varied from those of established non-IoT networked devices. The test array accuracy for all five methods attained 0.99. The testing methodology is shown in Fig. 5. These preliminary results motivate more research on anomaly detection in machine learning to safeguard IoT devices.

Damopoulos et al. [26] examine the significance of Intrusion Detection Systems (IDS) for mobile devices and the need of personalized files tailored for each user to establish an effective IDS for thwarting attacks. They evaluated many methods in the Phone activity dataset they constructed and documented the outcomes. The authors discovered that they could identify anomalies with considerable precision. They also gathered pertinent metrics for each algorithm used in mobile phone identification. Their primary objective was to develop IDSs compatible with the dataset, especially targeting anomalies.

Security Solutions For IOT

IoT security risks exploit vulnerabilities in several components, including applications and interfaces, network elements, and multiple tiers of software, firmware, and hardware devices. In the IoT paradigm, people interact with these components over potentially insecure protocols. We have delineated the security concerns associated with each IoT layer in this domain, along with their significance and the recommended remedies for each situation outlined in Section III.

This section analyzes the main security solutions that have been proposed. Table I provides a comparative examination of security risks and corresponding responses across the lowest, medium (transport layer), and highest levels. All threat factors, their consequences, and comparative assessments are considered.

A. Low-Level Security Solutions

Jamming attacks on Wireless Sensor Networks (WSN) include interference that results in message collisions or channel saturation. Young et al. [48] provide a technique for identifying jamming assaults by assessing signal quality, which facilitates the extraction of noisy data; this approach enables the detection of such attacks. Subsequently, for the purpose of attack detection, these numbers are juxtaposed against predetermined threshold values. Inaccurate MAC values may be used by a nefarious Sybil node to masquerade as an alternative device. This may result in resource depletion and the obstruction of access to sanctioned network devices. Demirbas et al. [49] provide a technique for detecting Sybil assaults using signal strength metrics. To ascertain the sender's location during message transmission, their solution utilizes detector nodes. A Sybil attack is suspected when a distinct message transmission originates from the same sender location but has a different sender identity. Measurements of MAC address signal intensity are used to detect spoofing attempts. The paper [30] delineates an approach for averting sleep deprivation assaults in wireless sensor networks (WSNs). The proposed design employs a cluster-oriented concept, whereby each cluster is subdivided into several sections. Minimizing long-distance communication reduces energy consumption. The framework employs a five-layer design for wireless sensor networks to execute intrusion detection.

IOT Architecture

Protocols are a set of instructions that facilitate the transmission and reception of data between electronic devices, according to pre-established agreements about data structure. IoT protocols are standards for data exchange and transmission over the internet and among devices. Various writers have suggested distinct IoT designs, including middleware-based architectures, Service-oriented architecture (SOA), as well as six-layer and three-layer architectures [17]. To resolve the core communication problem, we will concentrate on the essential three-layer IoT architecture shown in Fig. 1, which outlines the predominant protocols and standards used for powering IoT devices, applications, and systems. These three tiers include a "perception layer," a "network layer," and a "application layer":

The perception layer comprises physical and communication devices, including sensors and controllers, that gather, process, and refine information prior to its transmission to the network layer. It includes physical equipment like as cameras and Radio Frequency Identification (RFID) systems.

• The network and transport layer constitutes a communication tier employing gateways, switches, and routers to transmit and route data aggregated at the perception layer and delivered to the application layer. • The application layer serves as a communication layer housing the application responsible for user interaction. Each IoT layer utilizes a specific array of protocols and standards, as seen in Fig. 1. The protocols used by physical devices and communication technologies include Zigbee, Wi-Fi, 4G/5G, NB-IoT, and LoRaWAN. The network and transport layers use many protocols, including IPv6, 6LoWPAN, RPL, TCP, UDP, TLS, and DTLS. The communication and application protocols include XML, HTTP, MQTT, and CoAP. Furthermore, other protocols, such as OAuth 2.0, OpenID, and PKI, are used for key management and authentication [17, 18]. Figure 2 depicts a structured architecture based on the predominant IoT protocols for applications, including emailing,

authentication, key management, routing, and data transmission, as well as those pertaining to physical objects. The physical layer and the MAC (Media Access Control) layer are two fundamental levels delineated by the IEEE 802.15.4 standard. The physical layer standard pertains to data rates and frequency ranges for wireless communication channels. The MAC layer definition encompasses channel access mechanisms and synchronization. The Routing Protocol for Low Power and Lossy Networks (RPL) [19] facilitates IPv6 communication in low-power wireless personal area network (6LoWPAN) settings, allowing for connectivity and data transmission between several nodes and a central point; this standard also supports point-to-point traffic. The User Datagram Protocol (UDP) [20] is used in the IoT application architecture for communication due to its restricted payload capacity. The UDP protocol is seen as more efficient and less complex than the TCP protocol. Moreover, UDP header compression ensures the more efficient use of the limited payload space [21]. CoAP (Constrained Application Protocol) [22] delineates a framework for low-power, lossy networks operating in constrained environments predicated on demand response. Moreover, it facilitates asynchronous message transmission and may connect to IoT resources via HTTP mapping; LPWAN allows extensive connections of IoT devices. It offers low-power and low-bit-rate connection, in contrast to a wireless WAN that requires more energy to function at a high bit rate. LPWAN facilitates communication between gateways and end devices to regulate varying data rates.

Evaluation Methodology

The approach for evaluating IDS ML functioning in the IoT context, comparing accuracy results while considering efficiency. To implement machine learning, several algorithms were compared and their performance in the Intrusion Detection System was assessed using the assessment methodologies outlined below.

A. Performance Evaluation

Intrusion Detection Systems (IDS) provide alerts by identifying both typical behavioral patterns and potential attack scenarios. This behavior is classified as • True-positive (TP): The count of real assaults discovered.

• True-negative (TN): The quantity of standard activities identified as normal.

• False Positive (FP): (Intrusion Missed) The quantity of assaults identified as standard traffic.

• False-negative (FN): The quantity of normal activities misidentified as an assault.

Performance Analysis

This section demonstrates that the suggested protocol is appropriate for real-time applications in IoT systems.

A. Computational Efficiency

Given fixed block ciphers, the complexity of encryption and hash operations may be regarded as O(N), where N is the size of the message. Nonetheless, as shown in Section IV-C, the complexity of permutation creation is O(n log n), where n is the number of data batches in Pwindow. By analyzing these different difficulties, we can demonstrate that the difficulty of the seed sharing phase is O(N), but the complexity of the data transmission phase is O(N + n log n) for validation packets and O(1) for regular packets. Considering the dimensions of Pwindow, n is anticipated to fall between 15 and 25, resulting in minimal complexity. Nonetheless, using the conventional method of transmitting a MAC with each packet results in a data transmission phase complexity of O(N) for every packet. Furthermore, considering that N is less than n, we infer that the suggested procedure exhibits reduced computing complexity.

Scenarios to assess the efficacy of the suggested regimen. Initially, we maintain the MAC size in the conventional method and The hash size in the proposed system remains unchanged. In this instance, owing to the almost same packet size, we anticipate that the energy used by the radio will be equivalent for both the suggested and conventional methodologies. Nevertheless, since we compute the hash just for the validation packets, we anticipate that the proposed protocol would use less CPU resources in comparison to the conventional method. The CPU utilizes around 70% more energy in the conventional method with a MAC size of 256 bits. Furthermore, an augmentation of 64 bits in the MAC size leads to an escalation of about 2630 µJ in CPU energy for the conventional method, while the suggested protocol exhibits a little rise of 43 µJ in CPU energy. Figure 2 illustrates the CPU and radio energy consumption of both the suggested and standard protocols for this situation. The security of the proposed approach, as shown in Section V-A1, derives from the challenge of disrupting the random permutations. Consequently, we deem a 64-bit hash function adequate for the proposed protocol. Nevertheless, the majority of MAC systems need bigger MAC widths, often 128 bits or more, to provide equivalent security levels. In our second scenario, we maintain the hash size for the proposed protocol at 64 bits while changing the MAC size for the existing technique from 64 bits to 128 bits. In this instance, owing to the reduced packet size, we anticipate energy conservation not just for CPU use but also in radio energy consumption. The energy consumption of the CPU and the radio system. The CPU expends 41.51% more energy using the conventional method when the MAC size is 64 bits. The energy savings from the suggested protocol rise to 65% with a MAC size of 256 bits. Likewise, the suggested protocol may get up to 11.15% energy savings in the radio transceiver a comparison of the energy consumption between the suggested and existing approaches for the second scenario.

The findings indicate that the suggested method for identifying manipulated data and ensuring data integrity in IoT systems significantly reduces energy consumption compared to standard methods using MACs for data integrity.

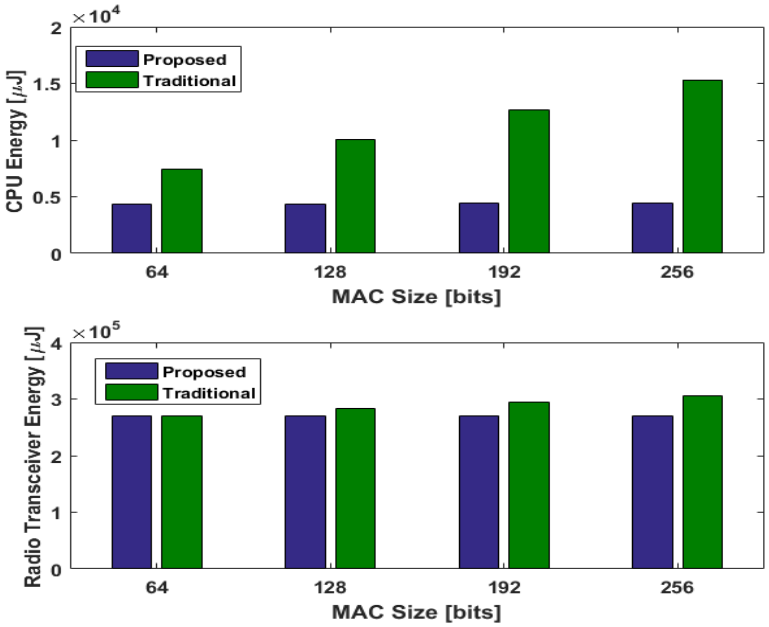

Fig. 2: Energy Consumed - Scenario

Conclusion

This work aims to provide an overview of several algorithms developed inside a limited context, ensuring the security of the IoT ecosystem. The research illustrated the use of supervised machine learning in the precise analysis of network traffic data for intrusion detection. It illustrated the method's efficacy in identifying significant traits to expedite training and testing durations. Particular applications concentrate on metrics. The objective was to determine the best effective classifier. This test provides conclusive metrics for the comparison of various algorithms. The findings illustrated the merits and demerits of each method used for anomaly-based intrusion detection systems.

Future Work

The expansion of the Internet of Things, characterized by several unique characteristics, has positioned IoT devices in a context where their standards and specifications markedly diverge from conventional solutions. The existing conventional solutions are inadequate for the IoT context. Moreover, the architecture of the IoT environment is often constructed using ARM architecture, which significantly differs from conventional x86 architecture. The fast expansion of IoT with distinct standards necessitates more research into effective security solutions applicable to the majority of IoT devices.

References

[1] ―System on a chip - Wikipedia.‖ [Online]. Available: https://en. wikipedia.org/wiki/System_on_a_chip. [Accessed: 12-Mar-2020].

[2] R. Roman, J. Zhou, and J. Lopez, ―On the features and challenges of security and privacy in distributed internet of things,‖ Comput. Networks, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: 10.1016/j.comnet. 2012.12.018.

[3]F. Alfaleh, H. Alfehaid, M. Alanzy, and S. Elkhediri, ―Wireless Sensor Networks Security: Case study,‖ 2019, pp. 1–4, doi: 10.1109/cais.2019.8769510.

[4] V. Chandola, A. Banerjee, and V. Kumar, ―Anomaly detection: A survey,‖ ACM Computing Surveys, vol. 41, no. 3. 01-Jul-2009, doi: 10.1145/1541880.1541882.

[5] N. Apthorpe, D. Reisman, and N. Feamster, ―A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic,‖ May 2017.

[6] F. Wortmann and K. Flü, ―Internet of Things Technology and Value Added,‖ Bus. Inf. Syst. Eng., doi: 10.1007/s12599-015-0383-3.

[7] L. Atzori, A. Iera, and G. Morabito, ―The Internet of Things: A survey,‖ Comput. Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[8] F. Samie, L. Bauer, and J. Henkel, ―IoT Technologies for Embedded Computing: A Survey,‖ doi: 10.1145/2968456.2974004.

[9] S. C. Ergen, ―ZigBee/IEEE 802.15.4 Summary,‖ 2004.

[10] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, ―A tutorial on IEEE 802.11ax high efficiency WLANs,‖ IEEE Commun. Surv. Tutorials, vol. 21, no. 1, pp. 197–216, Jan. 2019, doi: 10.1109/COMST.2018.2871099.

[11] ―Wi-Fi - Wikipedia.‖ [Online]. Available: https://en.wikipedia.org/wiki/ Wi-Fi. [Accessed: 14-Mar-2020].

[12] ―Connectivity Now and Beyond; exploring Cat-M1, NB-IoT, and LPWAN Connections.‖ [Online]. Available: https://ubidots.com/blog/ exploring-cat-m1-nb-iot-lpwan-connections/. [Accessed: 24-May-2020].

[13] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, ―A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications,‖ Feb. 2018.

[14] ―Threat Advisory: Mirai Botnet | Akamai.‖ [Online]. Available: https://www.akamai.com/us/en/resources/our-thinking/threat-advisories/ akamai-mirai-botnet-threat-advisory.jsp. [Accessed: 11-Nov-2019].

[15] J. Fruhlinger, ―The Mirai botnet explained: How IoT devices almost brought down the internet,‖ CSO Online, Mar. 2018.

[16] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, ―PHY-Layer Spoofing Detection with Reinforcement Learning in Wireless Networks,‖ IEEE Trans. Veh. Technol., vol. 65, no. 12, pp. 10037–10047, Dec. 2016, doi: 10.1109/TVT.2016.2524258.

[17] R. Halloush, ―Transmission Early-stopping Scheme for Anti-jamming over Delay-sensitive IoT Applications (IEEE Internet of Things Journal) Transmission Early-stopping Scheme for Anti-jamming over Delay-sensitive IoT Applications,‖ 2019, doi: 10.1109/JIOT.2019.2911683.

[18] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, ―Malware Threats and Detection for Industrial Mobile-IoT Networks,‖ IEEE Access, vol. 6, pp. 15941–15957, Mar. 2018, doi: 10.1109/ACCESS.2018.2815660.