2023

The Role of SOC in Ensuring the Security of IoT Devices: A Review of Current Challenges and Future Directions

Hajar Bennouri
Technological University Dublin, Ireland, hajar.bennouri@tudublin.ie

Abdiaziz Abdi
Technological University Dublin, Ireland, abdiaziz.abdi@tudublin.ie

Iqbal Hossain
Technological University Dublin, Ireland, iqbal.hossain@tudublin.ie

See next page for additional authors

The Role of SOC in Ensuring the Security of IoT Devices: A Review of Current Challenges and Future Directions

Hajar Bennouri*,1, Abdiaziz Abdi[1], Iqbal Hossain[1], and Alexandre Pujol[1]

[1]Collaboratory, Technological University Dublin, Ireland
*Correspondance: hajar.bennouri@tudublin.ie

2023 12th Mediterranean Conference on Embedded Computing (MECO) | 979-8-3503-2291-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/MECO58584.2023.10155021

***Abstract*—The growing popularity and deployment of Internet of Things (IoT) devices has led to serious security concerns. The integration of a security operations center (SOC) becomes increasingly important in this situation to ensure the security of IoT devices. In this article, we will present a summary of IoT device security issues, their vulnerabilities, a review of current challenges to keep these devices secure, and discuss the role that SOC can bring in protecting IoT devices while considering the challenges encountered and the directions to consider when implementing a reliable SOC for IoT monitoring.**

I. INTRODUCTION

In the 21st century, we can hardly do any services or business without an online presence. Despite the many benefits of online digital presence of businesses, we can see many incidents of online digital presence. We can see hackers constantly trying to hack data from companies and different services. It's like war; hackers are more active and smarter at stealing data. Cyberattacks can last a long time or for a short time, it can be overly sensitive government information as well as small private companies [1]. In addition, the massive evolution of connected objects in Internet of Things (IoT) environment that currently amount to more than 15 billion objects, and which is predicted to become more than 19 billion in 2025.

Hackers use a variety of tactics to attack organizations through the IoT, including loss of confidentiality, protocol and application integrity, authentication attacks, denial of service, access control, and physical security. An established security information and event management (SIEM) platform may already be in place in some organizations. Monitoring of IoT/CPS may already be planned for some large established enterprises, such as utilities and critical infrastructure. However, for small, medium, or new organizations, IoT deployment and strategic assessments may have only recently begun to determine the best approach to monitoring the security and safety of IoT devices being integrated into the IT infrastructure [2]. The development of IoT devices has had a substantial influence on a wide range of industries, including healthcare, transportation, manufacturing, and smart cities[3] [4] [5]. But nonetheless, the increasing usage of these devices has also raised serious security concerns regarding their vulnerability to hacking as well as other cyber threats.It is important to emphasize that the security of connected objects is a crucial issue insofar as it is at the heart of many sectors such as health, transport and industry. The consequences of a breach in the security of these devices could be disastrous, ranging from the loss of sensitive data to the danger of human life.

Security Operations Centers (SOCs) can provide a holistic solution to detecting and mitigating an attack if properly implemented [6]. SOC is a centralized department that continuously monitors, recognizes, and reacts to security problems. Security operations centres have grown in importance over the past 17 years, especially in the past five years.

While any SOC can mitigate various cyberattacks, some attacks that target an IoT environment cannot be mitigated by current SOC systems. The current SOC system is primarily designed for monitoring large databases, and the specific implementation has not taken direct interest and is designed for this type of environment. Security operations centers have become an essential element in this context to ensure the security of IoT devices. The use of the SOC to ensure that no internal or external threat compromises the security of IoT devices.[7], as the management of these connected objects becomes more and more essential and crucial in the face of cybercrime online which requires the implementation of a security management system for these objects.

This study examines possible offensive actions with the IoT, then takes a position on options for security operations center platforms. Start by making a complete inventory of IoT security based on existing research. In particular, we present the major challenges posed by the security of connected objects such as the diversity of devices, the protection of user privacy and the management of security updates.

We also discuss the methodologies used to mitigate security risks such as implementing encryption protocols, using firewalls, or adopting advanced security practices such as "bug bounty" or stress testing. penetration. We then present the existing SOC frameworks for IoT security, as well as It also examines the integration of IoT devices with the SOC and the function of the SOC in protecting critical infrastructure, insider threat reduction and implementation of a zero-trust architecture. The study goes on to describe the potential possibilities of SOC in IoT device security and explaining how these approaches could affect IoT security in the future. Regarding the challenges and opportunities ahead, this review article aims to give readers an in-depth understanding of the crucial role that SOC plays in

979-8-3503-2291-0/23/$31.00 ©2023 IEEE

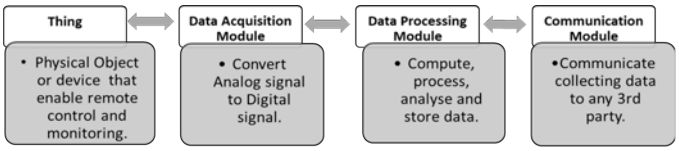

Fig. 1. Hardware 4 Building Blocks of IoT Devices

ensuring the security of IoT devices. Finally, we examine the future prospects for integrating a SOC into an IoT environment. We discuss the benefits that such a device could offer for the detection and prevention of security threats and we present future directions for a successful integration of a SOC in an IoT environment.

This paper is organized as follows. Section II presents related work of IoT security devices. Section III describes the IoT Security attacks, device vulnerabilities and potential countermeasures. Section IV introduces the SOC & IoT Integration Challenges and Section VI offers a general Discussion followed by our conclusions and future works.

II. IoT Security devices Literature Review

A. Hardware security perspective of IoT Devices

The Internet of Things (IoT) is based on intelligence and the ability of objects to communicate with each other and with computer systems to collect, analyze and share data. However, for this communication to take place smoothly and efficiently, the equipment used is essential. IoT sensors and processors must be designed to be powerful enough to process the data produced in real time,following the 4 hardware building Blocks of IoT Device as depicted in Figure 1 while being small and power efficient enough to be embedded in objects of all sizes and shapes.

The hardware security outlook of IoT devices is important, as most of these devices are often deployed in insecure environments and can be exposed to various types of threats. IoT devices are often designed with constraints in terms of cost, size, power consumption, and hardware resources, which can lead to potential vulnerabilities that can be exploited by attackers and can allow cybercriminals to take control of devices, steal data, intercept communications, or even cause physical damage.

Sidhu[8], pointed out that the security of IoT devices requires a secure hardware foundation. The article highlights several important points such as the importance of implementing hardware security for IoT devices, the challenges of securing hardware for these devices, as well as the threats to hardware and especially the introduction of the Hardware Trojan (HT). A detailed taxonomy of the hardware Trojan is provided, along with discussions of some insertion methods. Countermeasures are also offered, with an emphasis on HT detection techniques and design for trust.

In order to enhance the security of IoT devices, several approaches can be applied, including the use of secure chips, memory protection mechanisms, data confidentiality, integrity protection techniques, and device user authentication.When it comes to secure chips, these can offer mechanisms such as generating cryptographic keys, securely storing sensitive data, and securing communication between hardware components. Memory protection mechanisms can help prevent buffer overflow attacks and code injection attacks. Figure 2 illustrates the limitations of some hardware IoT devices, as well as potential attacks and associated defense mechanisms[9].

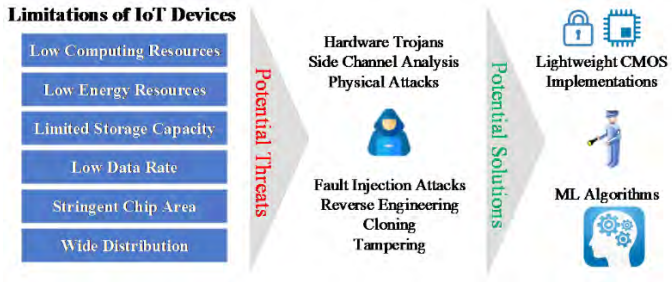

Fig. 2. IoT Devices hardware limitation,security threats and potential solutions[9]

B. IoT Architecture

IoT architectures bring together and harmonize all stages of detection and action on data coming from or sent to remote devices. In addition, this architecture must ensure the transmission and reception of messages as well as the storage, processing and analysis of data. To achieve the ultimate exploitation of data, IoT architectures make use of cloud, fog computing and edge computing, as well as services and other types of applications [10]. Different presentations are proposed in the literature for the IoT architecture, the most common used are the **Three Layer Architecture** and the **Five Layer Architecture** as presented in Figure 3.

Three Layer architecture is composed by the Application Layer, Network, and the perception Layer, that are defined as follow:

- *Perception Layer*: Sensing and sending/receiving Data
- *Network Layer*: responsible to ensure link and interconnectivity between IoT devices and other hardware devices.
- *Application Layer*: Provide specific application services that could be deployed by user.

The Five Layer Architecture have business, application perception, processing, and transport layers. (See Figure 3). The Perception and Application layers have the same role as in the Three layer architecture. We will describe the role of the three remaining layers.

- *Transport layer*: is mostly for Data routing and transmission
- *Processing layer*: For data aggregation module to ensure communication between transport layer and lower layers.
- *Business layer*: is business-oriented layer for providing operations management and data analysis tools to produce applications that help decision-making through.

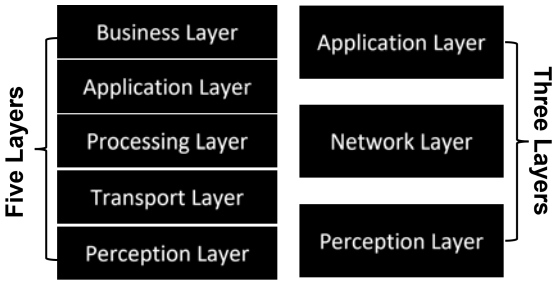

Fig. 3. Most known IoT Architectures: Three Layer and Five Layer Architectures

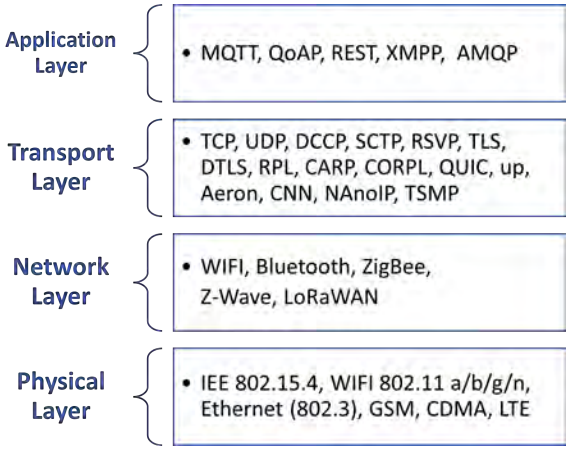

Fig. 4. IoT Communication Protocols following the 4-layer ISO architecture

C. IoT communication methods: limitation & advantages

The Internet of Things (IoT) universe involves the use of many protocols to enable communication and networking of connected devices. However, communication protocols are essential to create successful IoT networks. The choice of the best IoT protocol is based on various criteria such as the range of the targeted application, the energy consumption, the bandwidth and the latency of information, as well as the quality of service, while taking into account the security of the data. IoT devices rely on network standards and protocols to provide communication between connected objects through the cloud. Figure 4 present the different IoT Communication Protocols following the 4-layer ISO architecture.

These network protocols and standards have guidelines that define the rules for communication between different devices. Generally, each device is connected to the Internet via Internet Protocol (IP), as it can also connect locally via technologies such as Bluetooth, NFC (near field communication) or other technologies. Choosing the right communication protocol depends on the specific needs of the IoT application. For example, for applications that require real-time data transmission with low latency, it is important to select a protocol with high bandwidth and minimal latency. Conversely, for applications where power consumption is paramount, a low-power protocol should be preferred to extend battery life. Finally, security is a key concern in the choice of any IoT protocol, as connected devices can be vulnerable to computer attacks. For IoT devices, many challenges are encountered in terms of methods and protocols used to ensure secure communication between IoT devices and also with data collection stations.In the following we present some known protocols used in IoT communication regarding to each Layer.

For the application layer, many IoT communications protocol are used, mainly we can find:

a) CoAP and MQTT: The Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT). CoAP and MQTT are two communication protocols that are optimized for IoT devices and aim to minimize device power and bandwidth consumption. They both aim to minimize network overhead by using lightweight messages and reducing the size of message headers. Additionally, they both could process messages asynchronously, allowing efficient communication between devices that have limited resources in terms of processing power, memory, and power. However, CoAP mainly focuses on request-response type communications while MQTT is a publish-subscribe type messaging protocol[11]. MQTT allows devices to post messages about a particular topic, which can then be received by other devices subscribing to that topic.

b) AMQP: Advanced Message Queuing Protocol (AMQP) is an open source norm and one of the most reliable and secure protocols, so known for its scalability with minimal effort, on the other hand the major drawback of AMQP is that it has high memory requirements, with slow data transfer[12].

For the Transport layer, the main used protocol is TCP and UDP

c) TCP/IP: It is not possible to directly implement the Transmission Control Protocol and Internet Protocol (TCP/IP) stack on an IoT device because the maximum transmission unit (MTU) size of 1280 bytes in IPv6 may be too large for low-power devices that provide low MTUs [13]. Additionally, TCP provides various features, such as reliable transmission, flow control, and congestion avoidance, which may be too complex to implement on constrained IoT devices. Also, since IoT links can be loss-prone, TCP may not provide good performance, as it assumes that losses are only caused by congestion.

Regarding Network layer, many protocols and approaches are available in to ensure a secure communication for IoT devices, most of them are presented in what follow.

d) Wi-Fi: Wi-Fi is a wireless computer network technology set up to operate as an internal network and has since become a means of high-speed Internet access. It is based on the IEEE 802.11 standard [14] (ISO/IEC 8802-11). One of these advantages is that it is quite practical and easy to install, with a high data transfer rate, but on the other hand Wi-Fi is known for its energy consumption which is very high compared to what can provide a very small object, as well as the difficulty of scaling it to IoT Objects[15].

e) 6LoWPAN: It's an approach for routing Internet Protocol version 6 (IPv6) over low-power wireless networks defined by the Internet Engineering Task Force (IETF) standard. The first advantage of using the 6LoWPAN protocol [16] is its ability to work with a limited amount of RAM (Random Access

Memory), requiring only 4 KB. This software stack allows the activation of IPv6 and the User Datagram Protocol (UDP), thereby ensuring compatibility with various underlying physical (PHY) and Media Access Control (MAC) layers. Additionally, specifications have been developed to enable the transmission of IPv6 packets over IEEE 802.15.4 networks, routing, neighbour discovery, and header management algorithms, thereby enabling interoperability with IP networks. Finally, the 6LoWPAN stack supports packet fragmentation, reassembly, routing, neighbour discovery, multicast, and overhead compression of 2 to 11 bytes of TCP/UDP and IP headers, while supporting supports UDP and TCP transport protocols.

f) Zigbee: ZigBee is a wireless communication protocol using a specific network, based on the IEEE 802.15.4 standard [17]. This protocol has the particularity of being an open source protocol. The use of the ZigBee protocol ensures us the highest levels of security, with low energy consumption since it sends signals at very low frequency (2.4 GHz), it is also known for its long communication range. On the other hand, Zigbee remains a protocol exposed to interference and also an expensive protocol.

g) Z-Wave: Z-Wave uses low-power radio technology in the 868.42 MHz frequency band, which is faster than Wi-Fi or Bluetooth and offers low-power operation, but is still low in latency, with reasonable coverage. On the other hand Z-Wave has a low data transfer rate and is known to be premium priced [15].

h) LoRaWAN: LoRaWAN is a network protocol particularly suited to the development of the Internet of Things. It uses the LPWAN (Low Power Wide Area Network) communication model, it allows large-scale deployment (wide area), characterized by its scalability and wide network coverage for low energy consumption. On the other hand, its most known disadvantages are, its low data transfer rate and its personalized LoRa gateway[18].

i) BLIP: The Berkeley Low-power IP stack (BLIP) [19] is an open-source wireless sensor network protocol designed for low-power, low-memory IoT devices. BLIP offers an efficient solution for data communication in wireless sensor networks, providing a complete IP protocol stack with IPv6 support for addressing and connectivity. BLIP is optimized for low-power networks and uses data compression techniques to minimize power consumption and maximize battery life of IoT devices. Additionally, BLIP is easily adaptable to the various underlying physical and media access control layers, making it highly configurable and scalable for IoT applications.[20]

j) Thread: Thread [21] is a protocol used by IoT devices that incorporates an interface that conforms to the IEEE 802.15.4 PHY standard [22], along with additional support for a subset of the IEEE 802.15.4 MAC protocol. Thread uses the 6LoWPAN protocol for network communication. The low power consumption of IoT devices can result in weak transmission signals, making communication difficult. To ensure message privacy, Thread Personal Area Networks (PANs) use Datagram Transport Layer Security (DTLS) which is particularly suitable for wireless sensor networks, as it does not require a reliable transport layer, while guaranteeing security and data protection.

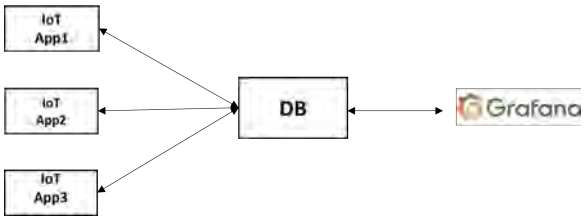

Fig. 5. Classic Monitoring Solution using Grafana

An example of protocol used in the Business Layer for monitoring data, we have:

k) Grafana: Grafana [23] is an open-source data analysis and visualization software that can be used to monitor and display data collected by connected objects. As for connected objects, Grafana can be used to monitor and visualize a wide variety of data, such as temperature, humidity, pressure, noise level, etc. It can also be used to track the status of various systems, such as sensors, actuators, controllers, etc. The Grafana platform provides alerting, notification, and collaboration functionality, as well as tools for creating custom charts and dashboards. It is compatible with many data types and protocols, which makes it a very flexible monitoring and data visualization tool for connected objects. An example of a Classic Monitoring Solution using Grafana is presented in Figure 5.

III. IoT SECURITY ATTACKS, DEVICE VULNERABILITIES AND POTENTIAL COUNTERMEASURES

A. Security Model

Depending of the use case of a IoT device, the security requirements may change from an IoT device to another. However; as any other computing device they usually share a common ground. These common security requirement is known as the CIA triad [24] and it can be sum up in:

- **Confidentiality:** A user can only read data it holds read permissions on.
- **Integrity:** A user can only write data it holds write permissions on.
- **Authentication:** A user can only access their data after the server has verified their identity.

This basic security requirements can easily be extended depending of the need. For example, the octave's security goal [25] also consist of assuring the following security properties:

- **Non repudiation:** A user cannot denies action it has done on a device
- **Auditability:** Each action on a device is logged
- **Accountability:** Each action can be traced back to the user that originated it
- **Trustworthiness:** Each action with third party client can be verified and a trust can established

However, IoT devices suffer from special constraints making the security possibly hard to ensure. This constrains of multiple type:

- **Hardware constraints:** Computational & memory limitation, ability to apply firmware update
- **Software constraints:** Security patches
- **Network constraints:** Network availability to provide security update

B. Attackers

In terms of potential attacks on IoT devices, it is important to consider the capabilities of the attacker. Here are the different categories of attackers to consider:

- A **remote attacker** with control over the external network on which is connected the IoT device. But without physical access to the system.
- An **untrusted user** with full control over the external network and with a valid credentials to access to a IoT device.
- An **untrusted administrator** with full control over the external network and the Iot device using a valid credentials to access it.
- A **local attacker** with access over the network and access to the hardware such as probes, TPM, firmware.

To give some context, a local attacker could steal the IoT device or could modify it in a way they gain total access of it. It is also important to understand that each type of attacker can use different methods to compromise an IoT device. This is why it is essential to consider all the possibilities and adopt suitable security measures to protect IoT devices against these different categories of attackers.

C. Attacks

IoTs are subjected to various threats and security vulnerabilities in different domains. In this paragraph we present the main security concern a IoT device face.

a) Spoofing Attacks: When an attacker has access on one of the device on the network, it can make every devices on the network think it is a legitimate IoT devices. This attack can be done using various technique such as IP address, ARP or DNS spoofing.

b) Data transmission: IoT devices may use a wide range of wireless protocol in order to transmit data. Even if the common protocol presented in Figure 4 are known to be secure, they may be implemented or configured incorrectly on devices that is power limited. This is a common concern on IoT security. Modern security always require modern encryption algorithm (Elliptic-curve cryptography (ECC), Homomorphic Encryption). However, a lot of IoT devices are not powerful enough to run these modern algorithms [26].

c) Device specificity: They are two categories of IoT devices. Attacks will varies depending of this and it is important to consider these differences when evaluating the security of these devices.

- Hight-end: Powerful devices with full network capabilities like a Raspberry Pi or a TV box.
- Low-end: Tiny device without a proper CPU but a microcontroller. These devices usually do not run modern operating system, which can affect their security and therefore make them more vulnerable to attack.

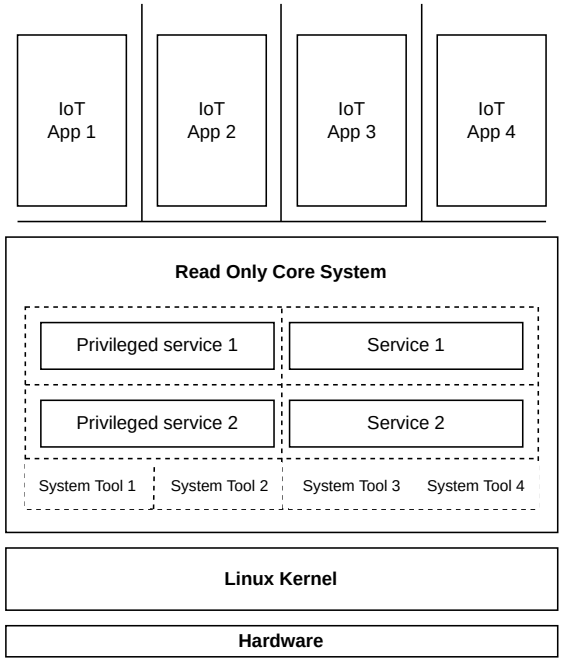

Fig. 6. Security Architecture of IoT based OS.

D. Solutions

After presenting the different attacks that may happen on IoT devices, this section presents the security construction usually used to ensure the security of devices to these attacks.

Multiple solution exist to ship IoT device with secured OS. We can cite projects such as: Ubbuntu Core[27], Fedora IoT[28], Yocto[29], BalenaOS[30], OpenEmbedded[31], and Buildroot[32]. They usually share a common ground. The core concept is that these OS are tailored for specific function and appliances. Therefore they can only run the few software they have been made for. Such a security construction provide a huge security benefit next to classic OS as it dramatically reduce the attacker surface and it makes running malware extremely complex from an attacker point of view. Figure 6 presents this security architecture, it consist of multiple layer. From the hardware to the IoT application, we have:

- The Linux kernel: it is compiled with only the necessary drivers to run on the target device.
- The core system: this is all the strictly necessary software and services to run the OS and to establish the network connection. It is immutable and can be cryptography verified at all time. This is useful for extending trust to the OS by mitigating zero days and unauthorized changes to root, as well as enforcing security policies, encryption and user-space security.
- The IoT application: The application that should run on IoT device are then split into different container. Each container has access to one type of resource (probe, sensors, network...)

Fig. 7. SOC Functional Components

IV. SOC & IOT INTEGRATION CHALLENGES

A. SOC Overview

A Security Operation Centre or Cyber Security Operation Centre is a setup where information security professionals collect, monitor, and respond while analyzing data to threats to protect the organization from cyberattacks. Additionally, the SOC consists of a very strong security concept with a number of strategically distributed security solutions throughout the organization. In a SOC there is even a series of processes and procedures to assess and maintain the security status of the company following the functional components as depicted in Figure 7.

In this section we will present the SOC, its functionalities, components and its role to detect, prevent cyberattacks as well as respond to cyberincidents.

1) Collection: The event monitoring and technology monitoring by SOC where it needs to collect information and generally this information is logs generated by the various components of the information system.

2) Analysis: The information collected is analyzed to determine any anomalies or incidents. This analysis requires log processing tools or using one of Security Information and Event Management (SIEM) tools.The analysis capabilities of SIEM systems can guide the reconfiguration of other enterprise security controls to close gaps in enterprise security and can detect attacks not found by other means. In the event that the attack is still ongoing, some of the best SIEM products can even prevent discovered security vulnerabilities. SIEM is additionally applicable for compliance reasons, such as user log activity or detecting unusual patterns of activity that may indicate a security threat. SIEM systems are frequently combined with many security tools like firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). Some of the most popular are: Arcsight ESM, IBM QRadar, and Splunk.

3) Monitoring: Security checks and investigations of various levels can be carried out by the SOC in this stage of monitoring. There are generally controls based on vulnerability scanners configured to analyze the vulnerabilities visible on the information system, make it possible to trace back to the SOC the state of security of IS assets, and to identify any vulnerabilities or threats. Other checks on compliance with technical standards make it possible to verify compliance with security policies, which may constitute as many subjects to be dealt with. Manual investigations or audits may also be performed by independent or SOC auditors. At the highest level of expertise, intrusion tests can be carried out in order to test the permeability of the systems without warning beforehand. At the end of this step SOC will Automatically create timelines for each detected anomalies.

4) Response: The last step concerns the optimization of detection rules for event collection using a SOAR (Security Orchestration, Automation and Response). The use of SOAR is very important as it helps automate workflows from the investigative path to start triage and then apply remediation processes in order to react in a more advanced way. This step can be automated thanks to the help of SOAR *playbooks*.

B. IoT Integration challenges

The significance of SOC in protecting IoT devices is thoroughly examined in this review study.[33] It examines the present issues that SOC faces in maintaining IoT security, as well as the future routes that SOC must take to overcome these challenges.[34] A review of current SOC frameworks for IoT security is also included in the paper, along with information on how IoT devices may be integrated with SOC and how machine learning and artificial intelligence are used to improve SOC for IoT security. Subsequently, the purpose of this review paper is to offer a thorough knowledge of the critical role that SOC plays in guaranteeing the security of IoT devices, as well as the challenges and possibilities that arise in the future.[10]

To defend enterprises against security threats, SOC teams are often made up of security analysts, incident response experts, and other security professionals. [35]They operate around the clock, continually monitoring network traffic and systems for abnormalities or security problems. When a security event is identified, SOC teams employ a variety of methodologies and technologies to investigate the event, mitigate the security breach, and patch any vulnerabilities that were exploited[33]. Table I outlining some of the challenges of IoT that should be taken in consideration while integrating these devises for security monitoring by SIEM.

C. Integration SOC for IoT monitoring

Monitoring IoT devices using a SOC implementation is described on Figure 8. In concept, it is similar to the classic monitoring solution detailed in Figure 5. Data is sent from IoT devices to a central database. Then the monitoring platform review the data and generate security events. The main addition here is the ability to automatically generate security response thanks to the use of a SOAR solution.

In order to integrate a SOC in a IoT platform, companies face some challenges toward a successful integration such as:

- Internal SOC resources that separate the IoT operation team from the computer infrastructure security team
- An integrated IoT/computer infrastructure SOC team

TABLE I
IOT INTEGRATION CHALLENGE

Study	IoT integration challenges	Description
[3]	Data management	Substantial amounts of data are produced by IoT devices, which can be difficult to manage and analyse efficiently. Efficient data management solutions are required to ensure timely and effective data processing.
[36]	IoT (Internet of Things) Security	IoT devices are vulnerable to internet-based threats that can lead to data breaches and potentially other security concerns. Security measures must be taken to protect both the devices and the data they collect.
[37]	Scalability	As the number of IoT devices in use increases, it can become difficult to monitor and maintain them all. Scalability is an issue that must be addressed for IoT systems to continue to function successfully as they grow.
[33]	Interoperability	IoT devices often come from different manufacturers and can use different protocols, making it difficult to integrate them into a single system. Interoperability standards are required for devices to communicate with each other.
[38]	Energy efficiency	Due to their battery-powered nature, many IoT devices may have limited performance and life expectancy. Devices need power management solutions to function for extended periods of time without having to be charged or replaced frequently.

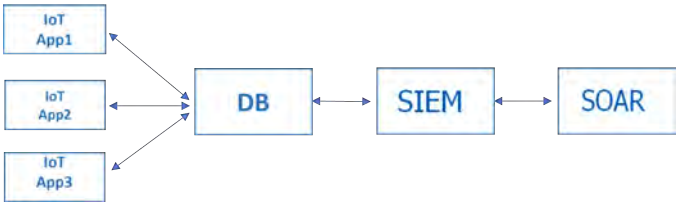

Fig. 8. SOC Monitoring Integration for IoT Devices

- Outsourced SOC (Managed Security Service Provider) that handles part or all the security elements

V. DISCUSSION & CONCLUSION

SOC is a technology that aims to ensure the security of an organization's computer systems and networks. Take advantage of this resource by integrating it into an IoT environment to ensure the identification of connected object systems, their protection and real-time monitoring to detect vulnerabilities and potential threats. The SOC may also be responsible for identifying threat actors likely to attack these objects, analyzing events and alerts to determine if they are associated with ongoing attack flows, triaging and investigating information, coordinate and respond to cyber incidents, and provide reporting and management information. The use of SOC will therefore play a crucial role in defending against computer attacks by proactively monitoring all connected objects in an IoT environment.

SOC technology can be used to solve many of the security issues that IoT devices encounter. To increase the security of IoT devices, SoC can include hardware and software-based security features, as well as encrypted communication methods. Despite the difficulties in integrating SoC into IoT devices, research in this area continues to provide encouraging results to further improve the security of IoT devices.

According to our study establishing a SOC for monitoring IoT devices requires several key steps to follow :

- Analyze security needs: It is important to determine the security needs for IoT devices in the organization. This can include vulnerability management, threat monitoring, protection against denial of service attacks, etc.
- Develop an IoT security strategy: An IoT security strategy must be developed to identify the security objectives and the measures to be taken to achieve them. This can include setting security policies for IoT devices, establishing security measures for IoT device data, access management, etc.
- Select the right security tools: It is important to select the right security tools for monitoring IoT devices. These tools can include IoT device security management solutions, intrusion detection tools, vulnerability management solutions, and more.
- Establish monitoring processes: Monitoring processes should be in place to monitor IoT devices in real time and detect potential threats. This can include setting up a dedicated monitoring team, defining threat detection protocols, etc.
- Set up a security event management (SIEM) infrastructure: A SIEM infrastructure can be set up to collect, analyze and correlate security data from IoT devices. This infrastructure can help identify potential threats and take action to counter them.
- Train staff: It is essential to train staff in managing the security of IoT devices and in the use of the security tools in place. This can help ensure that the Security Operations Center is effective in monitoring IoT devices.

On the whole, the investigations carried out on the security of connected objects have brought to light a cutting-edge analysis of this complex problem. However, it is unfortunate that this investigative work has not addressed the effectiveness of using a SOC to detect and prevent intrusions and threats to these devices.

This paper therefore fills this gap by delving into a wide range of challenges inherent in the security of connected objects. We also present the methodologies used to mitigate security attacks while integrating a SOC to monitoring devices in a IoT environment. Future research should focus on building hardware-based trust protocols, intelligent security systems, and secure device control.

REFERENCES

[1] Manfred Vielberth, Fabian Böhm, Ines Fichtinger, and Günther Pernul. Security operations center: A systematic study and open challenges. *IEEE Access*, 8:227756–227779, 2020.

[2] David Weissman and Anura Jayasumana. Integrating iot monitoring for security operation center. In *2020 Global Internet of Things Summit (GIoTS)*, pages 1–6. IEEE, 2020.

[3] Kamran Shaukat, Talha Mahboob Alam, Ibrahim A Hameed, Wasim Ahmed Khan, Nadir Abbas, and Suhuai Luo. A review on security challenges in internet of things (iot). In *2021 26th international conference on automation and computing (ICAC)*, pages 1–6. IEEE, 2021.

[4] Lo'ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. Iot privacy and security: Challenges and solutions. *Applied Sciences*, 10(12):4102, 2020.

[5] Abid Ali, Abdul Mateen, Abdul Hanan, and Farhan Amin. Advanced security framework for internet of things (iot). *Technologies*, 10(3):60, 2022.

[6] Hesamaldin Jadidbonab, Hoang Nga Nguyen, Siraj Ahmed Shaikh, Marcin Hlond, Peter Robertson, and Gajinder Panesar. A hardware-based soc monitoring in-life solution for automotive industry. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, pages 637–642, 2022.

[7] Tejasvi Alladi, Vinay Chamola, Biplab Sikdar, and Kim-Kwang Raymond Choo. Consumer iot: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine*, 9(2):17–25, 2020.

[8] Simranjeet Sidhu, Bassam J Mohd, and Thaier Hayajneh. Hardware security in iot devices with emphasis on hardware trojans. *Journal of Sensor and Actuator Networks*, 8(3):42, 2019.

[9] Emmanouel T. Michailidis, Dimitrios G. Kogias, and Ioannis Voyiatzis. A review on hardware security countermeasures for iot: Emerging mechanisms and machine learning solutions. In *24th Pan-Hellenic Conference on Informatics*, pages 268–271, 2020.

[10] Pierfrancesco Bellini, Paolo Nesi, and Gianni Pantaleo. Iot-enabled smart cities: A review of concepts, frameworks and key technologies. *Applied Sciences*, 12(3):1607, 2022.

[11] Samer Hamdani and Hassan Sbeyti. A comparative study of coap and mqtt communication protocols. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–5, 2019.

[12] Joel L. Fernandes, Ivo C. Lopes, Joel J. P. C. Rodrigues, and Sana Ullah. Performance evaluation of restful web services and amqp protocol. In *2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 810–815, 2013.

[13] G Yedukondalu. Challenges in i o t communication via transmission control protocol/internet protocol architecture. *constraints*, 6(9), 2017.

[14] Guido R. Hiertz, Dee Denteneer, Lothar Stibor, Yunpeng Zang, Xavier Perez Costa, and Bernhard Walke. The ieee 802.11 universe. *IEEE Communications Magazine*, 48(1):62–70, 2010.

[15] Gollu Appala Naidu and Jayendra Kumar. Wireless protocols: Wi-fi son, bluetooth, zigbee, z-wave, and wi-fi. In *Innovations in Electronics and Communication Engineering: Proceedings of the 7th ICIECE 2018*, pages 229–239. Springer, 2019.

[16] Geoff Mulligan. The 6lowpan architecture. In *Proceedings of the 4th workshop on Embedded networked sensors*, pages 78–82, 2007.

[17] MC13226V1 MC13226V LGA and MC13226VR21 MC13226V LGA. Advanced zigbee™-compliant platform-in-package (pip) for the 2.4 ghz ieee® 802.15. 4 standard. 2005.

[18] Adeiza J Onumanyi, Adnan M Abu-Mahfouz, and Gerhard P Hancke. Low power wide area network, cognitive radio and the internet of things: Potentials for integration. *Sensors*, 20(23):6837, 2020.

[19] TinyOS. Blip tutorial, available online. http://tinyos.stanford.edu/tinyos-wiki/index.php/BLIP_Tutorial. Accessed on March 24, 2023.

[20] Arslan Musaddiq, Yousaf Bin Zikria, Oliver Hahm, Heejung Yu, Ali Kashif Bashir, and Sung Won Kim. A survey on resource management in iot operating systems. *IEEE Access*, 6:8459–8482, 2018.

[21] Hyung-Sin Kim, Sam Kumar, and David E Culler. Thread/openthread: A compromise in low-power wireless multihop network architecture for the internet of things. *IEEE Communications Magazine*, 57(7):55–61, 2019.

[22] Andreas F Molisch, Kannan Balakrishnan, Chia-Chin Chong, Shahriar Emami, Andrew Fort, Johan Karedal, Juergen Kunisch, Hans Schantz, Ulrich Schuster, and Kai Siwiak. Ieee 802.15. 4a channel model-final report. *IEEE P802*, 15(04):0662, 2004.

[23] Mainak Chakraborty and Ajit Pratap Kundan. Grafana. In *Monitoring Cloud-Native Applications: Lead Agile Operations Confidently Using Open Source Software*, pages 187–240. Springer, 2021.

[24] Hezam Akram Abdul-Ghani and Dimitri Konstantas. A comprehensive study of security and privacy guidelines, threats, and countermeasures: An iot perspective. *Journal of Sensor and Actuator Networks*, 8(2):22, 2019.

[25] Waseem Iqbal, Haider Abbas, Mahmoud Daneshmand, Bilal Rauf, and Yawar Abbas Bangash. An in-depth analysis of iot security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet of Things Journal*, 7(10):10250–10276, 2020.

[26] Pintu Kumar Sadhu, Venkata P Yanambaka, and Ahmed Abdelgawad. Internet of things: Security and solutions survey. *Sensors*, 22(19):7433, 2022.

[27] Canonical. Ubuntu core. https://ubuntu.com/core/. Accessed on March 24, 2023.

[28] Fedora. Fedora iot. https://getfedora.org/iot. Accessed on March 16, 2023.

[29] Yoctoproject. https://www.yoctoproject.org/. Accessed on March 16, 2023.

[30] Balena os. https://www.balena.io/os. Accessed on March 16, 2023.

[31] Openembedded. https://www.openembedded.org. Accessed on March 16, 2023.

[32] Buildroot. https://buildroot.org/. Accessed on March 13, 2023.

[33] David Weissman and Anura Jayasumana. Integrating iot monitoring for security operation center. In *2020 Global Internet of Things Summit (GIoTS)*, pages 1–6, 2020.

[34] R Somasundaram and Mythili Thirugnanam. Review of security challenges in healthcare internet of things. *Wireless Networks*, 27:5503–5509, 2021.

[35] Wiem Bekri, Taher Layeb, JMAL Rihab, and Lamia Chaari Fourati. Intelligent iot systems: security issues, attacks, and countermeasures. In *2022 International Wireless Communications and Mobile Computing (IWCMC)*, pages 231–236. IEEE, 2022.

[36] Junyoung Jung, Jinsung Cho, and Ben Lee. A secure platform for iot devices based on arm platform security architecture. In *2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, pages 1–4. IEEE, 2020.

[37] Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke, and Pete Burnap. Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology*, 4(3):125–152, 2020.

[38] Partemie-Marian Mutescu, Adrian Ioan Petrariu, and Alexandru Lavric. Wireless communications for iot: Energy efficiency survey. In *2021 12th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, pages 1–4, 2021.