Computing&AI Connect
ISSN: 3104-4719
2024, Article ID. 2024.0004, Cite as: https://doi.org/10.69709/CAIC.2024.193182

SCIFINITI

Review Article

OPEN ACCESS

An Overview of Secure Network Segmentation in Connected IIoT Environments

Vishnu Vardhan Baligodugula **Ashutosh Ghimire** **Fathi Amsaad***

Department of Computer Science and Engineering, Wright State University, Dayton, OH 45435, USA

Article History
Submitted: June 18, 2024 Accepted: August 8, 2024 Published: August 28, 2024

Abstract
Network segmentation is a very important approach in enhancing network security. The approach involves breaking down the network into smaller, more manageable segments, each with its own specific security requirements. This strategy supports maintaining stable perimeters and effective access control while safeguarding critical resources, such as database servers, from unauthorized access. The relevance of network segmentation in IIoT comes with the state-of-the-art and interconnected nature of many devices that may pose extensive safety issues. To address these challenges, the Secure IIoT Network Segmentation Framework was developed as a specialized cybersecurity solution for IIoT environments. This framework includes specific guidelines for growing custom designs that improve safety posture and protect essential records. In IIoT environments, security segmentation is crucial for keeping different business structures separated, each with its own specific protection requirements, and for safeguarding them against the unique risks posed by interconnected devices. Specific problems of the access factors pose precise problems in IIoT networks because they function as convergence nodes for lots of devices, therefore making sure to provide many types of privacy breaches and interactions with different firms. Segmentation provides many benefits, which include accelerated protection, a reduced attack surface, simplified compliance, and improved device management. Still, it also complicates things and adds operational overhead, and there are fee concerns as well. Apart from community segmentation, a lot of techniques have been practiced to reinforce the safety framework: Federation of IDs, Micro-segmentation, Firewall, Network Access Control (NAC). It provides control of unique visitors, enforces security regulations, and deals with community access while supporting segmentation efforts and enhancing universal safety in IIoT structures. One such relevant approach with respect to network segmentation, more particularly in IIoT environments, concerns the enhancement of safety, protection of sensitive statistics, and compliance with enterprise requirements. By using frameworks like SiNeSF and complementing protection techniques, an organization can set up secure obstacle building, access limitation, and hazard restriction on the risks related to networked IIoT devices.

Keywords:
Industrial Internet of Things (IIoT); SINeSF; network segmentation; user access restrictions; security measures

1. Introduction

The strategic process that intends to break down a network into smaller segments often to reinforce safety is called network segmentation. This can be achieved through segmentation, which will help isolate internal user traffic. Compared with external visitors and contacts, this approach provides better control over who has access to the community [1]. This segmentation lets in discrete areas for specific operations, which include net servers, databases, and team of workers devices, making it less complicated to regulate protection zones. Segmentation ensures compliance with regulatory requirements, protects sensitive data from insider threats, and makes it more difficult to access insecure devices. Although community segmentation can provide advantages beyond protection, including general performance optimization, this article focuses on its shielding functions [1].

In the Industrial Internet of Things (IIoT), community segmentation is crucial as a couple of gadgets engage in the identical community. The complexity of IIoT has led to extensive security vulnerabilities, as seen by the

* **Corresponding Author:**
Fathi Amsaad, Department of Computer Science and Engineering,
Wright State University, Dayton, OH 45435, USA; fathi.amsaad@wright.edu

explosion of denial-of-service attacks focusing on those devices [2]. This paper explains the network segmentation pattern, specifically the Abstract Security Pattern (ASP), and then distinguishes between IIoT segmentation patterns. The ASP outlines the conceptual and semantic restrictions of a domain, shielding it from threats without focusing on implementation specifics. It also provides a framework for managing regulatory risks [3]. Real-world case studies will demonstrate practical implementations of information security, emphasizing the crucial necessity for IIoT segmentation as a strong framework for protection. Furthermore, the discussion will differentiate between hierarchical identification patterns and segmentation strategies applicable to both IIoT and traditional non-IIoT scenarios, including network service segmentation [4].

The structure of this paper is as follows. Section 2 provides an overview of the IIoT architecture; Section 3 explores comprehensive IIoT security principles and strategies; Section 4 reviews related works in the field; Section 5 outlines proposed strategies for network segmentation within connected IIoT environments; and Section 6 focuses on IIoT security segmentation, culminating in a conclusion that highlights the key benefits of implementing network segmentation within IIoT frameworks.

The IIoT itself is defined as a network of interconnected devices designed for data collection and exchange, primarily aimed at optimizing industrial processes. IIoT architecture is generally categorized into four essential layers. Edge devices, gateways, data management and cloud, each serving a unique function in the global data processing and handling ecosystem, as illustrated in the accompanying Figure 1.

1.1. Edge Devices in the Internet of Things

The Internet of Things (IoT) network is fundamentally anchored by the device layer, which functions as the initial layer where various interconnected devices are located at the network's edge. This layer is primarily composed of industrial Internet of Things (IIoT) devices strategically deployed in proximity to the data source to ensure efficient information gathering. The devices typically involve remote sensors, and coupled with this are actuators that play very critical roles in data acquisition and control processes. Each cluster of devices is fitted with a processing unit or even a lightweight computing device, which enables local computations, accompanied by a range of monitoring.

In the IoT area, one may additionally come across a wide variety of gadgets. These range from legacy devices working inside brownfield environments to advanced IoT sensors, robot cameras, microphones, and numerous meters and video display units. The primary function of IoT sensors is to capture information from the surrounding environment or from specific objects under observation. Upon collecting this information, sensors process and convert it into usable facts that may be analyzed via human beings or other structures.

In addition to sensing, the actuator element is important for handling and manipulating the physical approaches that occur within the monitored environment. Actuators are responsible for performing actions based on the received data, thereby adjusting the conditions under which measurements are taken. For example, an actuator can additionally manage the opening or closing of a valve, or it can manage a mechanical arm during automatic assembly line operation. This interaction between sensors and actuators not only enhances the efficiency of data collection but also ensures that the monitored environments can be dynamically regulated, ultimately facilitating a more responsive and intelligent IoT ecosystem. Consequently, the machine layer is imperative to set up the muse for powerful facts conversation and operational automation within IoT networks.

1.2. IIoT Segmentation Security

Safety segmentation in the IIoT environment of commercial systems lends itself to the isolation of a wide diversity of companies within IIoT systems and their related additives that address several security requirements for each unit. Nowadays, the IIoT landscape has the mixing of a heterogeneous set of devices with different origins, types, and security postures. This immense interconnectivity introduces risks that are not normally anticipated in conven-

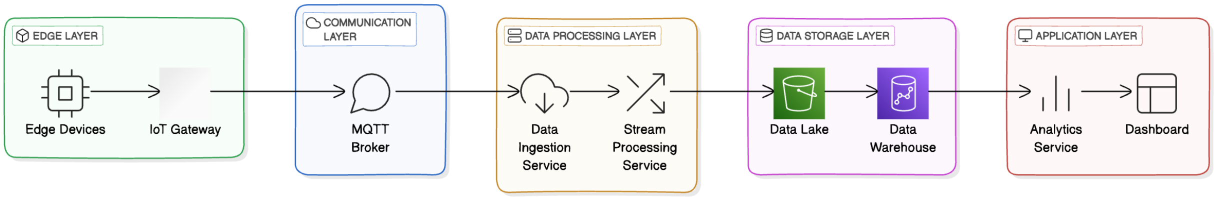

Figure 1: IIoT Architecture Layers: A Simplified Diagram.

tional tool training. The access factors, which provide interconnection nodes for lots of devices, are at the heart of this complexity. These access points often lack adequate privacy protections and frequently communicate with external agencies over the internet, which can create complex situations that pose significant security risks.

Sensor networks are one of the most important addins for any cyber-physically-based system (CPS) device that has major threats to human safety and belongings. The network is an ubiquitous platform for the operational procedures in IIoT devices, and fog computing layers enhance their performance skills. Although fog computing incorporates dispersed sub-layers that provide help to quit devices, this abstraction also introduces new vulnerabilities inside massive-scale interconnected systems. Protecting the critical tools from the systems-related attacks is difficult, mainly because of the heterogeneity of the sources, formats, security schema, and computational capabilities of those devices. The complexity of those systems can also bring conflicts in terms of access and manipulation, which accordingly complicates the strategies to control.

Network segmentation offers numerous benefits in its implementation but also presents significant challenges. In addition, this separation of sensitive information and critical systems from the broader campus enhances security by minimizing the chance of access and capability breaches. This also reduces the attack surface, which means a reduced number of vulnerable sites and thus lesser chances of successful cyberattacks. Segmentation of the network helps to maintain compliance with the requirements of a regulation by only allowing specific access to sensitive documents and systems. This improves device management, clearly defining responsibilities for each device to enhance overall security and operational efficiency.

On the other hand, the implementation of the community segmentation can bring additional complexity that requires careful planning and continuous control to keep a robust structure. Operational overhead can result from segmentation, as it may introduce latency and performance degradation if not managed carefully. In addition, the implementation of a powerful segmentation approach regularly involves cost considerations; companies can also need to spend money on additional hardware and software solutions, which leads to accelerated monetary burdens.

However, deploying network segmentation can be a complex task due to the need for extensive logistical planning and strategy to maintain and operate such a system effectively. One of the consequences of imposing expenditure is that it can spark latency and performance degradation if it is wrongly managed. In addition, the strategy of segmentation also has cost considerations in its implementation. It may require organizations to spend more money to acquire more equipment and software, and that alone can prove very expensive.

Segmentation can be maximized through the use of different methods and other techniques that are associated with the subject. One of them is federated identities, which is a technique that offers a means to dynamically and securely manage identities across segments and systems within an organization. Another strategy is microsegmentation, which enables control of data traffic within subgroups, thus, security is improved by eliminating the possibility of attacks on other parts of the network. The use of firewalls and NAC (Network Access Control) systems is also paramount in the enforcement of security policies, as well as the management of access not only at the network perimeter but also within the structure of the internal organization Through the application of these techniques, companies can set up a strong security structure that will help to reduce the threats which arise from the heterogeneous and intricate nature of IIoT environments.

2. Partitioning IIoT Segmentation

Partitioning the industrial Internet of Things (IIoT) network into many segments, each including trusted devices behind more secure partitions, is a sensible approach to managing IIoT networks. A typical arrangement is shown in Figure 2, where fog computer systems and organizational equipment are clearly divided into segments.This methodical technique improves the management of information streams and the security organization. To realize the fundamental confinement inside Local Area Networks (LANs), switches and Virtual Local Area Networks (VLANs) play a basic part. Gadgets interface to the haze computing design, which in turn interfaces to the bigger organizational arrangement and the cloud, as outlined in Figure 2. This division essentially reinforces the overall security posture of the IIoT network, which is crucial for protecting sensitive information and ensuring that each segment can be independently monitored and managed.

2.1. Key Factors Influencing IIoT Segmentation

Several factors influence the successful implementation of security segmentation in IIoT environments:

- **Heterogeneity:** IIoT networks comprise a wide variety of devices with different security requirements. Managing and controlling the participation of these diverse devices in the network is essential.

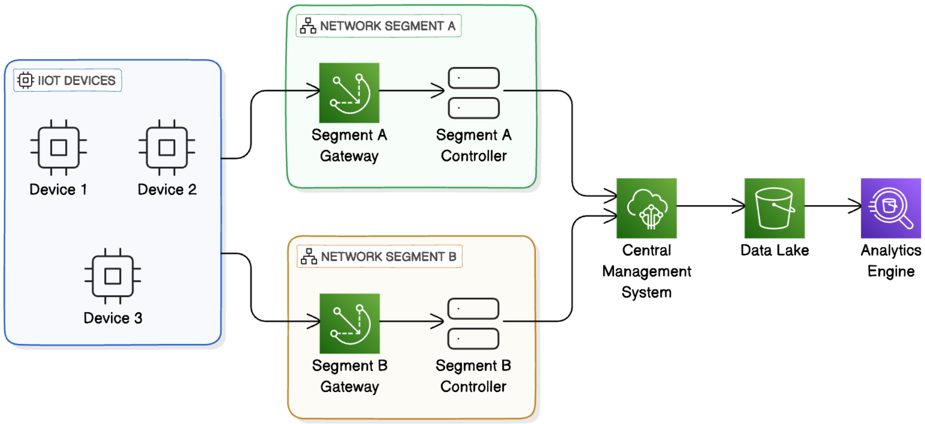

Figure 2: A Partitioned Network of IIoT Connected Devices.

- **Identity Management:** Due to the large number of devices, robust identification and management systems are necessary to ensure each device is properly monitored and controlled.
- **Standardization:** Establishing consistent security standards across cloud, fog, and edge devices is critical to maintaining a secure IIoT environment.
- **Attack Surface Reduction:** Segmenting devices based on their risk profiles helps reduce the overall attack surface of the IIoT network.
- **Compliance:** Compliance with security regulations becomes more manageable with effective segmentation, ensuring that policies are applied uniformly across different device types and network segments.
- **Threat Management:** Given the critical nature of IIoT systems, effective segmentation is essential for managing and mitigating security threats effectively.

2.2. IIoT Gateways

In IIoT situations, portals play an important role as central centers where IoT sensor information is collected, digitized, and handled recently being transmitted to the cloud. The portals are set near to the sensors and actuators, encouraging pre-processing assignments at the edge. This approach reduces latency and bandwidth usage by filtering and aggregating data locally before transmission. With portals, the management of the IoT data that comes from the sensors can be extremely challenging. They convert the original low-resolution sensor signals into digital data that is suitable for AI to learn from and analyze. Besides this, the recent advancements in portals may include self-diagnostics and built-in security tools to assess and protect incoming data streams in real-time.

2.3. IIoT Network Segmentation

Effective segmentation in IIoT means implementing some strategies against the exact challenges of these environments.

- **Segmented VLANs:** Segment different classes of devices into different VLANs, with very strict security policies attached to them.
- **Captive Portals:** Implement captive portals for the guest network and devices for implementing access control based on authentication.
- **Traffic Monitoring:** Use advanced monitoring tools and techniques to monitor the traffic of IIoT networks in order to rapidly identify and respond to anomalies.
- **Unique Device Identification:** Come up with secure ways to uniquely identify and authenticate every IIoT device.

Several solutions proposed prove real-world effective IIoT segmentation strategies:

- **Arctic Wolf IIoT Segmentation:** Tailored solutions by Arctic Wolf that are aimed at enhancing the security of IIoT environments.
- **Tempered Networks Layered Security:** The solutions provided by Tempered Networks ensure transparent and secure connectivity across layered IIoT systems.
- **Pluribus SDN Segmentation:** Pluribus Networks harnesses Software-Defined Networking to implement and manage effective segmentation in IIoT networks.

2.4. Benefits and challenges of IIoT Segmentation

The main advantages that arise among others from implementing segmentation into the IIoT environment are numerous.

- **Enhanced security:** Segmentation, to some extent, restricts devices' and their data movement. Therefore, this will reduce the chances of any unauthorized access in general, thus improving the security of the large network.
- **Enhanced Compliance:** The segmentation process helps an organization to abide by the different regulatory requirements; for example, it allows the application of security policies as required.
- **Reduced Complexity:** Proper segmentation strategies make management and securing of a wide array of IIoT devices easier.
- **High performance:** This segment reduces latency and enhances the network performance by way of controlling traffic and access.

Despite the advantages, IIoT segmentation presents some challenges to its implementation:

- **Complexity:** A huge device array and implementing efficient strategies of segmentation can be complex and resource-intensive.
- **Integration Issues:** The already existing security standards and patterns are hard to be integrated into the IIoT environments because of the variety of devices and systems involved in it.
- **Operational Overhead:** Its implementation and continued additional hardware, software, and the management effort that goes on are required for segmentation. It increases the operational cost.

2.5. Data Management Layers

Processing starts at the sensor level, and this is useful when information is needed immediately. In this context, edge computing is crucial for achieving fast responses by processing data locally at the edge of the network. It enables preliminary processing directly where the data is generated, such as at IIoT sensors, which are positioned at the edge of the network [5]. The method begins once sensor information is captured, digitized, and totaled, making it appropriate to encourage examination through edge IT frameworks. These edge IT frameworks may be either on-premise or remote; in any case, they are regularly arranged in nearness to the sensors to optimize proficiency. At this point, the digitized and totaled information is utilized for analytics purposes, empowering the application of machine learning algorithms and data visualization methods. The insights extracted from this processed data are then prioritized for transmission, instead of sending all collected information to centralized information centers or cloud stages. It is a concentrated approach that reduces the amount of data in motion, hence eliminating concerns about capacity, security, and the potential for downtime. Edge preparation of information enables organizations to drive operational efficiency and decision steps on the back of easily digestible chunks of information, hence effectively managing information strategies.

2.6. Cloud Computing

Edge devices are constrained in their capacity to perform broad pre-processing, requiring dependence on cloud computing for more profound examination and bits of knowledge. The primary objective is to perform as much processing as possible at the edge to conserve local computational resources. However, for complex computations, cloud services become essential. The primary objective is to perform as much processing as possible at the edge to conserve local computational resources. However, for complex computations, cloud services become essential. This doubles the focus on leveraging the speed characteristic of edge computing whereas tapping into the broad explanatory capabilities of cloud stages. In cloud environments, data collected from various sources undergoes integration and analysis, providing insights that are not easily achievable at the edge, particularly for industrial process management.

High-quality data management, storage, and analysis are facilitated by cloud servers, on-premises data centers, or hybrid systems. These cloud servers possess the computational power necessary for thorough and secure data analysis, although the trade-off is longer processing times. Yet, in the cloud computing space, there is more focus on data analytics by pulling together insights from multiple data streams which then creates novel knowledge that contributes to operational efficiency.

The IIoT solution is organized into a series of layers, where each level is meant for cloud setups or edge devices, and it works perfectly as the system deals with data processing, analysis, and collection. A thorough understanding of these layers helps the firms to improve their operational processes and to solve some specific security problems that appear at every layer. Working on these key issues gives companies the opportunity to fully use IIoT, resulting in smarter and more efficient industrial operations. Comprehension of this enables not only the improvement of workflows but also the strengthening of security measures, and as a result, the businesses remain competitive in a technology landscape that is rapidly evolving.

3. Principles and Strategies of IIoT Security

The Industrial Internet of Things (IIoT) security scene can be inspected through two critical areas: Nonexclusive security necessities and particular challenges at different design layers. Adherence to the foundational standards of confidentiality, integrity, and availability (CIA) is basic; be that as it may, a few challenges complicate the realization of these targets [3].

3.1. Generic IIoT Security Requirements

- **Confidentiality**: Ensure that the access of information is guaranteed to be accessible only to authorized entities and prevent any unauthorized access and leakage, especially for sensitive information handled by devices of the IIoT [6].
- **Integrity**: Preserve the accuracy and reliability of the information exchanged between platforms and adopt counter measures in case of unauthorized modification of data, which ensures uniformity in data [7].
- **Availability**: This dimension seeks to ensure timely access to data and hardware resources for the operational requirements of IIoT applications in order to improve the user experience.
- **Authentication**: Define mechanisms that would enable devices to securely authenticate each other and verify the identity of agents trying to access IIoT systems, to prevent unauthorized control [8].
- **Lightweight Encryption**: Consider mechanisms of encryption that work with the low processing capabilities of IIoT devices, to ensure secure transmission of information without sucking all available power resources [9].
- **Policy and Standards Compliance**: Design policies and Security policies that manage, protect, and transmit data. Establishment of compliance mechanisms builds trust and accelerates the growth of the IIoT ecosystem.
- **Encrypted Key Management**: Lightweight key management systems that can efficiently allow the establishment of trust and distribution of keys with respect to the trade-off between security needs and device resource constraints [10].

3.2. Specific Security Challenges by Layer

- **Hardware Constraints**: IIoT devices often possess limited processing power and memory, making it difficult to implement rigorous and advanced security solutions.
- **Computational Limitations**: Many IIoT devices cannot support demanding encryption and security protocols due to their low computational capability [11].
- **Fragmented Ecosystem**: Due to the breadth and heterogeneous nature of IIoT systems, managing security cohesively is challenging. The devices have huge differences in specifications and functionalities [1].
- **Performance Issues**: With the massive deployment of IIoT nodes, these can become performance bottlenecks, therefore, resource management and optimization strategies are efficient only if they consider all of them [12].
- **Conceptual Challenges**: A set of unique operational requirements of IIoT systems contribute to complexities in establishing secure connections and communication channels.

3.3. Strategies for Strengthening IIoT Security

- **Software Security**: Deploy approved security solutions across all IIoT devices to shield against vulnerabilities [13].
- **Authentication on Network Access**: Mandate that devices authenticate their identity upon network connection before any data exchange occurs [2].
- **Firewall Implementation**: Use firewalls to filter inbound and outbound data packets. This offers greater security even in the event of resource-constrained situations [3].
- **Periodic Updates**: Update devices with the latest security patches for vulnerabilities. In doing this, consider both the requirement for updating and bandwidth constraints [4].

Briefly, managing the challenges of IIoT security requires a general approach that must include the standards of design securely, appropriate strategies for resource-constrained cases, and proactive management of the security practices throughout the lifecycle of devices. The further development of standards and specifications will be the key to efficient and effective protection of the emerging scene of IIoT.

4. Network Segmentation in Connected IIoT Environments

Network segmentation is one of the most important security measures for Industrial Internet of Things (IIoT) contexts, and it includes the logical or physical segmentation of a network into isolated segments. In this way, an advanced form of policy enforcement and security threat monitoring is permitted. This section describes different approaches and best practices for effectively implementing network segmentation in connected IIoT contexts [14].

4.1. Guidelines for Network Segmentation in IIoT Environments

Operational efficiency with robust security in IIoT environments can be found on a few of the following central tenets:

1. **Security Level:** This is the labeling of entities across a network regarding type, influenced by data sensitivity and isolation from other entities to avoid unauthorized access.
2. **Attack Surface Reduction:** The idea here is to minimize the quantity of exposed endpoints at every segment, thus drastically reducing the opportunities for security breaches.
3. **Management of Heterogeneity:** Device heterogeneity from different manufacturers needs to be addressed with a clear policy of segmentation to reduce associated risks.
4. **Identity Management:** End-to-end identity management that ensures comprehensive tracking. This includes connected devices, hence helping in access to sensitive segments only by authenticated devices.
5. **Compliance:** Bring segments in line with regulatory provisions by making access to sensitive data limited.
6. **Threat Containment:** Minimize the impact of breaches by ensuring that threats remain within specific segments and do not move on to the whole network.
7. **Overhead Consideration:** Balance security measures with operational complexity; in other words, bring in efficiency while enhancing security.

4.2. Implementing Network Segmentation

Network segmentation can be effectively carried out using several techniques illustrated in Figure 3.

4.2.1. Segmentation Techniques

Network segmentation can be accomplished using the following facilities.

- **Physical Segmentation:** The isolation of segments through physical infrastructure separation [2].
- **Virtual Segmentation:** Design of logical isolated segments using virtual local area networks [4].
- **Firewall Rules:** Advanced and high-level firewall rules configured to control the flow of traffic between such segments [9].
- **Access Control Lists:** ACL configuration to manage device and user access to such segments [15].
- **Network Access Control:** Using NAC solutions to enforce the access policies based on device compliance [16].
- **Micro-segmentation:** Fine-grained policies are implemented at the level of individual workloads or applications that will limit the lateral movement of threats [17].

4.2.2. IIoT Implementation Scenarios

Figure 3 shows a sequence diagram for one of the use-case scenarios, which addresses the requirement for accessing a sub-network in a segmented IIoT setup. All of these segmentation use cases can be taken into account with regard to certain specific requirements, such as security, scalability, and operational efficiency in actual field applications.

- **Payment Card Industry Compliance:** Segmentation of network segments allows keeping the sensitive Card Holder Information safe from probing for access in any manner other than secure channels [6].
- **Healthcare Networks:** It isolates patient data by separating the systems for the management of medical records from the other components of a network.
- **Manufacturing Systems:** Protecting critical OT from less secure IT networks ensures the integrity of production processes.

5. IIoT Security Segmentation

5.1. Benefits, Challenges, and Security Mechanisms of Network Segmentation

Network segmentation is the vital point in the modern cybersecurity environment that allows organizations to reap many benefits along with some obstacles that they have to tackle. One of the main benefits of network segmentation is that it strengthens security. By separating necessary systems and confidential data, organizations can almost en-

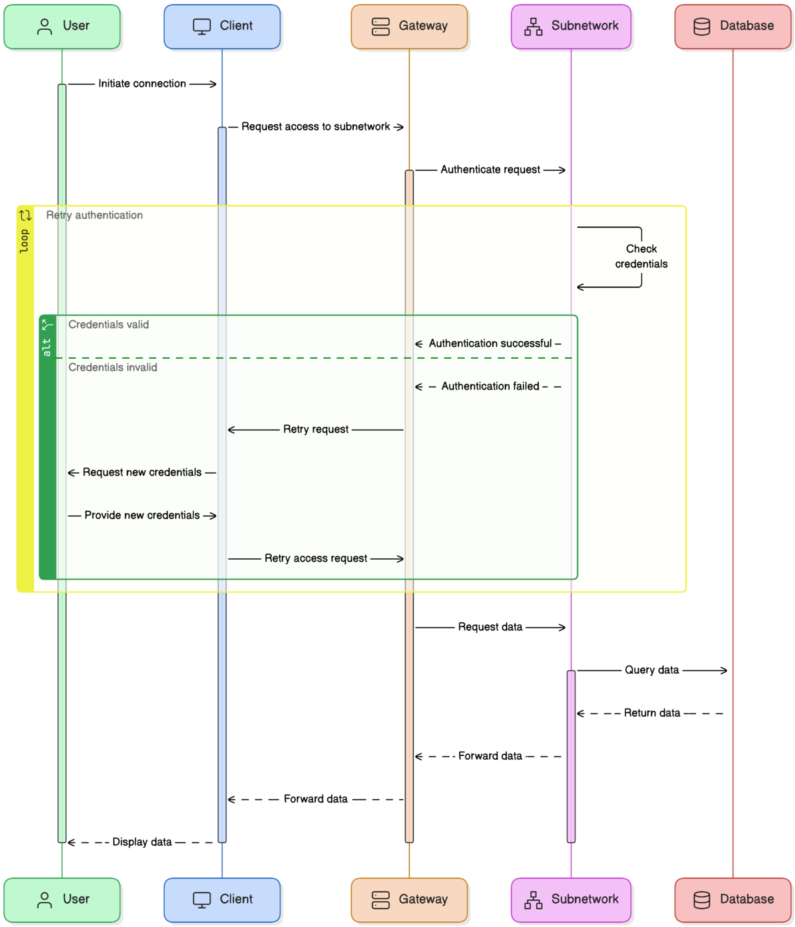

Figure 3: Sequence Diagram: Accessing a Subnetwork Example.

tirely avoid violations of breaches [16]. Through this separation, the exposure of the attack surface is reduced, thus the number of endpoints that may be in the face of a possible threat is minimized. In turn, the probability of successful cyberattacks is reduced [18]. Additionally, with segmented networks, compliance with various regulatory standards becomes more manageable. Segmentation allows organizations to clearly define the boundaries of their networks and restrict access to specific areas, thereby aiding in meeting legal requirements [19]. Device management which is the effective control of devices is also made possible through segmentation, as it makes clear the identity and function of each device, thus, the overall control and visibility on the network is improved.

Nevertheless, with all of these attractive features, organizations still face numerous problems in their adoption of network segmentation as shown in Table 1. The most important of these is the complication of network architecture, which now has to be planned very carefully and managed all the way so that the segmentation will be effective. Segmentation that is not properly managed may lead to operational overheads, which, in turn, may be the reason for latency and performance issues that will affect business operations [20]. Besides, the implementation of segmentation often comes with extra costs since organizations might have to purchase new hardware and software to be able to support this strategy leading to the rise of operational expenditures. In order to overcome these hindrances and fully maximize the advantages of segmentation, institutions can use different security techniques [21]. For example, federating identities can ensure secure identity management across different segments while microsegmentation limits the possible attack vectors and enhances traffic control within those segments. Alongside traffic firewalls and NAC systems, deploying NAC can also assure the compliance of security policies as well as control the access. Also, guaranteeing that the segmentation is not only the protection of the network but is also correctly working as it should be [19].

Table 1: Benefits, Challenges, and Security Mechanisms of Network Segmentation.

Type	Item	Description
Benefits	Enhanced Security	Protects sensitive data by isolating critical systems.
	Reduced Attack Surface	Minimizes exposed endpoints, lowering attack success chances.
	Simplified compliance	Aids in adherence to regulatory mandates by restricting access.
	Improved Device Management	Clarifies device identity and role, enhancing overall control.
Challenges	Increased Complexity	Requires careful planning and ongoing management.
	Operational Overhead	Potential latency and performance issues if mismanaged.
	Cost Considerations	Additional hardware/software may raise expenses.
Security Mechanisms	Federation of IDs	Ensures secure identity management across segments.
	Micro-segmentation	Enhances traffic control within segments, limiting attack vectors.
	Firewall and NAC	Enforces security policies and controls access effectively.

6. Implementing IIoT Segmentation

6.1. Overview

Proper strategic segmentation of IIoT networks is crucial for effective management. By creating distinct partitions within the network, organizations can identify and isolate trusted devices, placing them in secure segments. This approach enhances data flow management and overall security through segmented control. An ordinary scenario of such community partitioning is illustrated in Figure 4, which highlights how organizational systems and fog computing structures are divided into isolated segments. Within Local Area Networks (LANs), devices such as switches and Virtual Local Area Networks (VLANs) play an extensive position in maintaining up this separation. Gadgets are associated with both fog and larger organizational structures, eventually finding their way back to cloud infrastructure—the greater reason being department in the defense of data integrity.

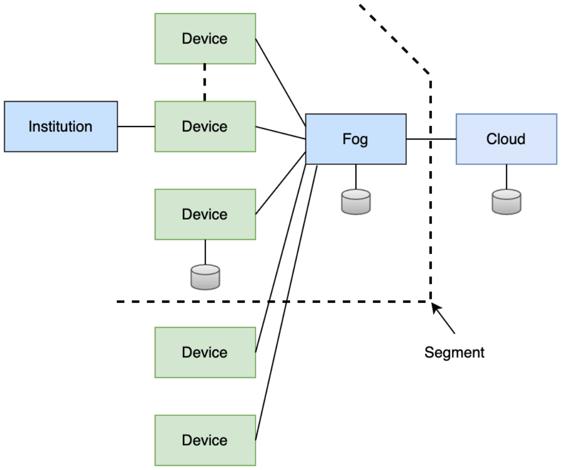

Figure 4: A Segmented Network of IIoT Devices.

6.2. Key Factors Influencing Segmentation

IIoT Segmentation will be successful if the critical factors identified in Table 2 are followed below.

6.3. Implementation Strategies

The following methods can be used to effectively segment the IIoT:

- **VLAN Segmentation:** Different, individual VLANs for each device type; each is associated with specified security policies.
- **Captive Portals:** Deploy captive portals on guest networks, forcing authentication.
- **Traffic Monitoring:** Implement next-generation traffic analysis tools for real-time traffic visibility, monitoring for anomalies.
- **Unique Device Identification:** Implement secure IIoT device identification and authentication.

6.4. Practical Solutions

Real-world implementations that show effective IIoT segmentation strategies are included in Table 3.

6.5. Benefits of Segmentation

The implementation of segmentation in IIoT has the following application-based benefits:

- **Advanced Security:** The isolation of the devices reduces the chance of unauthorized access.
- **Better Compliance:** This helps an organization provide an entity with consistency in policy application to meet compliance needs.
- **Reduced complication:** It makes the management process and security for various devices easier.
- **High Performance:** The control on network traffic actually reduces latency and improves throughput.

Table 2: Key Factors for IIoT Segmentation.

Factor	Description
Heterogeneity	IIoT networks contain diverse devices with varying security needs, necessitating effective management.
Identity Management	A robust system for device identification is essential for monitoring and controlling network access.
Standardization	Consistent security standards across all devices and networks ensure a cohesive and secure environment.
Attack Surface Reduction	Segmenting based on risk profiles minimizes the overall vulnerability of the network.
Compliance	Effective segmentation aids in meeting regulatory requirements uniformly across device types.
Threat Management	Proper segmentation is vital to identify and mitigate security threats within the system.

Table 3: Practical IIoT Segmentation Solutions.

Solution	Description
Arctic Wolf Segmentation	Tailored solutions designed to enhance IIoT security.
Tempered Networks Security	Ensures transparent and secure connectivity across layered systems.
Pluribus SDN Segmentation	Utilizes Software-Defined Networking for effective network management.

6.6. Challenges of Implementation

Despite the benefits, IIoT segmentation faces a number of challenges enumerated in Table 4.

To mitigate the challenges of IIoT segmentation, an approach must be structured and best-practice-based with an approach designed specifically to handle the unique security requirements of IIoT environments. This will ensure that all the features that come with segmentation are still retained but with the effectiveness of managing security on organizational networks.

7. Conclusion

Dividing a network into smaller manageable segments helps to boost security. This approach known as network segmentation plays a key role in protecting networks. This paper has taken a deep look at IIoT network segmentation highlighting why it matters and the best ways to secure IIoT systems.

The segmentation pattern that has been discussed lay the groundwork. It brings together key functions that could be tweaked to fit the specific needs. This basic pattern is not set in stone. Instead, it kicks off the creation of a series of linked patterns. These expanded patterns build on the main ideas of segmentation, which leads to big steps forward in keeping IIoT networks safe and well managed. By putting network segmentation into action, companies can keep different parts of their IIoT systems separate. This separation cuts down the chances of people getting in when they shouldn't and limits how much damage they can do by keeping security threats in specific areas. Also, each area has its own security rules and ways to control who gets in. This makes it easier to watch what is going on and helps stop threats from spreading, leading to a stronger network setup.

The ability to customize is at the heart of the segmentation method. Companies can adjust the segmentation patterns to meet their specific needs and issues offering a flexible and adjustable structure. As new tech and

Table 4: Challenges of IIoT Segmentation.

Challenge	Description
Complexity	Management of diverse devices and strategies can be resource-intensive.
Integration Issues	Ensuring consistent security standards across heterogeneous systems poses difficulties.
Operational Overhead	Additional hardware and software, along with ongoing management, can increase costs.

gadgets pop up, this basic pattern gives a strong base to build extra security steps and management techniques on.

It could be deduced that IIoT network segmentation brings big benefits by cutting down on weak spots making monitoring better, and allowing custom security rules for different parts. This method can keep up with tech progress and company changes making it easy to scale up.

List of Abbreviations

AI	Artificial Intelligence
IoT	Internet of Things
IIoT	Industrial Internet of Things
LANs	Local Area Networks
ML	Machine Learning
VLANs	Virtual Local Area Networks
ASP	Abstract Security Pattern
CPS	Cyber-Physically-based System
NAC	Network Access Control

Authors' Contributions

V.V.B. and F.A. conceptualized the core ideas and framework of the paper. V.V.B. conducted the primary research and contributed to the initial drafting of the manuscript. A.G. outlined the structure of the survey and provided critical revisions to enhance the overall quality of the content. F.A. provided significant supervision and expert guidance throughout the process. All authors have read and approved the final version of the manuscript.

Conflicts of Interest

The authors declare no conflicts of interest regarding this manuscript.

Funding

This research was funded by the Air Force Research Laboratory (AFRL) Grant, under the Assured and Trusted Digital Microelectronics Ecosystem (ADMETE) grant number BAA-FA8650-18-S-1201, awarded to Wright State University, Dayton, Ohio, USA. This project was carried out under the CAGE number: 4B991 and DUNS: 047814256.

Acknowledgments

This work was sponsored by the Air Force Research Laboratory (AFRL) Grant, under the Assured and Trusted Digital Microelectronics Ecosystem (ADMETE) grant BAA-FA8650-18-S-1201, awarded to Wright State University, Dayton, Ohio, USA. This project was carried out under the CAGE number: 4B991 and DUNS: 047814256.

References

[1] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for internet of things security," in Proceedings of the 2014 Euro Med Telco Conference (EMTC), November 12–15, 2014, Naples, Italy. pp. 1–5. Available at: https://www.proceedings.com/content/024/024777webtoc.pdf

[2] K. Gupta, A. Pandey, L. Chan, A. Yadav, B. Staats, and M. A. Borkin, "Portola: A hybrid tree and network visualization technique for network segmentation," in Proceedings of the 2022 IEEE Symposium on Visualization for Cyber Security (VizSec), October 19, 2022, Oklahoma City, OK, USA. pp. 1–5. Available at: https://virtual.ieeevis.org/year/2022/paper_a-vizsec-7865.html

[3] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan, "Industrial internet of things driven by sdn platform for smart grid resiliency," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 267–277, 2019. [CrossRef]

[4] B. Alotaibi, "A survey on industrial internet of things security: Requirements, attacks, ai-based solutions, and edge computing opportunities," *Sensors*, vol. 23, no. 17, 2023. [CrossRef] [PubMed]

[5] A. A. Mirani, G. Velasco-Hernandez, A. Awasthi, and J. Walsh, "Key challenges and emerging technologies in industrial iot architectures: A review," *Sensors*, vol. 22, no. 15, 2022. [CrossRef] [PubMed]

[6] E. Shaikh, I. Mohiuddin, and A. Manzoor, "Internet of things (IoT): Security and privacy threats," in Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), March 19–21, 2019, Riyadh, Saudi Arabia. pp. 1–6. [CrossRef]

[7] M. Ur Rahman, B. Vishnu Vardhan, L. Jenith, and V. Rakesh Reddy, "Spectrum sensing using nmlmf algorithm in cognitive radio networks for health care monitoring applications," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 5, pp. 1–7, 2020. [CrossRef]

[8] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "Iot security: Ongoing challenges and research opportunities," in Proceedings of the 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, November 17–19, 2014, Matsue, Japan. pp. 230–234. [CrossRef]

[9] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011. [CrossRef]

[10] K. Zhao and L. Ge, "A survey on the internet of things security," in Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, December 14–15, 2013, Emei Mountain, China. pp. 663–667. [CrossRef]

[11] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scal-

able iiot critical infrastructures in industry 4.0," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2300–2317, 2020. [CrossRef]

[12] H. Singh, V. V. Baligodugula, and F. Amsaad, "Shrew distributed denial-of-service (ddos) attack in iot applications: A survey," in *Internet of Things. Advances in Information and Communication Technology*, D. Puthal, S. Mohanty, and B.-Y. Choi, Eds. Cham: Springer Nature Switzerland, 2024, pp. 97–103. [CrossRef]

[13] A. Ghimire, V. V. Baligodugula, and F. Amsaad, "Power analysis side-channel attacks on same and cross-device settings: A survey of machine learning techniques," in *Internet of Things. Advances in Information and Communication Technology*, D. Puthal, S. Mohanty, and B.-Y. Choi, Eds. Cham: Springer Nature Switzerland, 2024, pp. 357–367. [CrossRef]

[14] B. Li, Y. Zou, R. Zhu, W. Yao, J. Wang, and S. Wan, "Fabric defect segmentation system based on a lightweight gan for industrial internet of things," *Wireless Communications and Mobile Computing*, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:249024329.

[15] Y. Zhang, C. Yang, K. Huang, and Y. Li, "Intrusion detection of industrial internet-of-things based on reconstructed graph neural networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2894–2905, 2023. [CrossRef]

[16] N. Mhaskar, M. Alabbad, and R. Khedri, "A formal approach to network segmentation," *Comput. Secur.*, vol. 103, p. 102162, 2021. [CrossRef]

[17] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013. [CrossRef]

[18] V. V. Baligodugula, F. Amsaad, V. V. Tadepalli, V. Radhika, Y. Sanjana, S. Shiva, S. Meduri, M. Maabreh, N. Alsaadi, O. Darwish, A. Razaque, and Y. Tashtoush, "A comparative study of secure and efficient data duplication mechanisms for cloud-based iot applications," in *Proceedings of the 2023 International Conference on Advances in Computing Research (ACR'23)*, K. Daimi and A. Al Sadoon, Eds. Cham: Springer Nature Switzerland, 2023, pp. 569–586. [CrossRef]

[19] M. Oqaily, Y. Jarraya, M. Mohammady, S. Majumdar, M. Pourzandi, L. Wang, and M. Debbabi, "Segguard: Segmentation-based anonymization of network data in clouds for privacy-preserving security auditing," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 5, pp. 2486–2505, 2021. [CrossRef]

[20] M. Alabbad, N. Mhaskar, and R. Khedri, "Two formal design solutions for the generalization of network segmentation," *J. Netw. Comput. Appl.*, vol. 222, p. 103763, 2024. [CrossRef]

[21] S. Jeuk, G. Salgueiro, F. Baker, and S. Zhou, "Network segmentation in the cloud a novel architecture based on ucc and iid," in Proceedings of the 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), October 5–7, 2015, Niagara Falls, ON, Canada. pp. 58–63. [CrossRef]