Vol. 7, No. 2, August 2025, pp. 113~127, p-ISSN 2685-2381, e-ISSN 2715-2626
http://dx.doi.org/10.28989/avitec.v7i2.2918

# A Combined Approach to Safety and Security of IoT by Applying Fault Tree Analysis and Attack Trees with Minimal Cut Sets

**Mohammad Rezaul Karim[1]*, Sohag Kabir[2], Ci Lei[3], Raluca Lefticaru[4], and Mohammad Abdul Baset[5]**
[1,2,3,4]School of Computer Science, Artificial Intelligence and Electronics
Faculty of Engineering and Digital Technologies, University of Bradford, United Kingdom
[5]Department of Textile Engineering
Faculty of Mechanical Engineering, Dhaka University of Engineering and Technology, Bangladesh

**Article Info**

**Article history:**
Submitted March 10, 2025
Accepted May 2, 2025
Published May 9, 2025

**Keywords:**
Internet of Things;
Safety;
Security;
Minimal Cut Sets;
Fault Tree Analysis.

**ABSTRACT**

The rapid proliferation of Internet of Things (IoT) systems introduces complex safety and security challenges, as traditional frameworks often treat these aspects separately, overlooking critical interdependencies. This study proposes a unified methodology integrating Fault Tree Analysis (FTA) and Attack Trees (AT) with Minimal Cut Sets (MCS) to holistically assess IoT safety and security. FTA systematically identifies root causes of system failures, while AT models attack vectors and their probabilities. By deriving MCS—minimal combinations of safety faults and security breaches—the approach reveals critical scenarios where failures and attacks interact, enabling prioritized mitigation. Applied to a real-world IoT dataset (BoTNeTIoT-L01), the framework identified key vulnerabilities, such as Data_Corruption (safety probability: 0.005) linked to Mirai attacks (security probability: 0.01), demonstrating how integrated MCS enhance risk visibility. Quantitative analysis (mean safety: 0.005, variance: 0.000006) confirmed the methodology's effectiveness in capturing interdependencies across IoT layers (Perception, Network, Data Processing, Application). Results emphasize that combined safety-security analysis prevents isolated risk assessments, offering actionable insights for resilient IoT design. The study concludes that integrating FTA-AT-MCS bridges existing gaps in IoT dependability, enabling targeted resource allocation and adaptive strategies against evolving threats. This approach advances IoT ecosystems' safety, security, and trustworthiness in interconnected environments.



**Corresponding Author:**
Mohammad Rezaul Karim,
School of Computer Science, Artificial Intelligence and Electronics
Faculty of Engineering and Digital Technologies, University of Bradford,
West Yorkshire, BD7 1DP, United Kingdom
Email: *rezabd9@gmail.com

## 1. INTRODUCTION

The rapid proliferation of the Internet of Things (IoT) has ushered in an era of unprecedented technological advancements, transforming the way interconnected devices communicate and operate [1]. Across diverse domains such as healthcare, transportation, and smart infrastructure, the integration of IoT systems has become pervasive, offering unparalleled opportunities for efficiency, automation, and data-driven decision-making [2]. As IoT continues to evolve and permeate various facets of daily life, it concurrently introduces complex challenges, with paramount importance placed on ensuring the safety and security of these interconnected ecosystems [3][4].

In the realm of critical infrastructures, industries, and daily routines, the profound impact of IoT systems necessitates a holistic and integrated approach to address both safety and security comprehensively [5]. Traditional methodologies often compartmentalize safety and security as distinct considerations, potentially overlooking the intricate interdependencies between the two [6]. As a response to this dichotomy, this research advocates for a paradigm shift—an approach that unifies Fault Tree Analysis (FTA) [7] and Attack Trees (AT) [8] with the derivation of Minimal Cut Sets to create a consolidated framework for assessing and enhancing the safety and security posture of IoT systems [9].

The Need for Integration: Given the interconnected nature of IoT devices, a compromise in either safety or security could have far-reaching consequences. The proposed integration of FTA and AT offers a novel solution to this challenge [10]. FTA, a proven methodology for evaluating safety vulnerabilities, is complemented by AT, a structured approach to assessing security risks. Combining these methodologies provides a unified representation, acknowledging the symbiotic relationship between safety and security within an IoT system [11].

Minimal Cut Sets as a Key Concept: At the heart of this integrated approach lies the concept of Minimal Cut Sets. Derived from both safety and security analyses, Minimal Cut Sets represent the minimal combinations of events that could lead to identified vulnerabilities [12]. This innovative concept enables a granular understanding of critical paths within the system, pinpointing specific components or events that, if compromised, could have cascading effects on both safety and security [13][14]. The identification of Minimal Cut Sets becomes instrumental in prioritizing mitigation strategies, ensuring a targeted and efficient response to potential risks [15].

Addressing Existing Limitations: The proposed methodology seeks to address the limitations of existing approaches that often meet safety and security assessments. By integrating FTA and AT with Minimal Cut Sets, this research aims to bridge the gap between safety and security considerations, providing a nuanced understanding of the risk landscape in IoT systems [16].

### 1.1 Novel Contributions

This research makes significant contributions to the field by advocating for a holistic approach to IoT safety and security. The subsequent sections will delve into the intricacies of the methodology, its practical application, and the potential transformative impact on the future landscape of IoT safety and security. Through this comprehensive examination, we aim to lay the foundation for a robust framework that advances the resilience and security of IoT ecosystems, addressing the evolving challenges posed by an increasingly interconnected world.

The novel contributions of this study are:

1. We integrate FTA and AT for a holistic safety and security assessment of IoT.
2. We develop methodology to derive Minimal Cut Sets (MCS) for efficient risk mitigation.
3. We apply the proposed approach to real-world IoT scenarios to validate its effectiveness.

### 1.2 Literature Review

Abdulhamid et al. (2022) [17] assessed the current status and challenges of the dependability of the Internet of Things (IoT). They systematically reviewed the current state and challenges associated with IoT dependability frameworks. The review revealed that most existing IoT dependability frameworks rely on informal reliability models. These models are inadequate for effectively assessing the unified treatment of safety faults and cyber-security threats in IoT systems. Furthermore, the current frameworks struggle to address the conflicting interactions between co-located IoT devices and the dynamic characteristics of self-adaptive, reconfigurable, and other autonomous IoT systems. Consequently, this paper proposes the development of a new model-based dependability framework to quantify safety faults and cyber-security threats, as well as the interdependencies between safety and cyber-security within IoT ecosystems. Additionally, there is a need for robust methods to manage conflicting interactions between co-located IoT systems and the dynamic behaviours of IoT systems in reconfigurable and other autonomous environments.

Kriaa et al. (2019) [18] developed a framework for safety and security joint risk analysis for industrial control systems. S-cube, which stands for supervisory control and data acquisition safety and security joint modelling, is an innovative model-based method that facilitates the formal representation of the physical and functional architecture of cyber-physical systems. This is achieved through a knowledge base, allowing for the automatic creation of both qualitative and quantitative analyses that cover safety risks (accidental) and security risks (malicious). Initially, we explain the principles and reasoning behind S-cube, followed by a demonstration of its inputs and outputs through a case study.

Ihirwe et al. (2023) [19] presented an early safety analysis approach based on Failure-Logic Analysis (FLA) and Fault-Tree Analysis (FTA) for safety-critical IoT systems. The safety analysis framework, bolstered by the CHESSIoT tool, evaluates the system-level physical architecture model, which is annotated with the failure logic properties of components, to conduct various automated failure analyses. Beyond its capability to generate system Fault-Trees (FTs), the novel FTA analysis method automatically carries out both qualitative and quantitative analyses. This includes removing redundant events and unnecessary failure paths, as well as automatically calculating the probability of undesired events. To evaluate the approach's effectiveness, a comparative study was conducted, contrasting our proposed method with 19 existing approaches from both academia and industry, highlighting its contribution to the field. Lastly, a Patient Monitoring System (PMS) use case was developed to showcase the capabilities of the CHESSIoT tool, with the results being comprehensively presented.

In Abbas et al. [20] (2022), the machine learning (ML) technique is considered the most advanced and promising method and opened up many research directions to address new security challenges in the cyber-physical systems (CPS). This research survey delineates the architecture of Internet of Things (IoT) systems, scrutinizes various attacks targeting these systems, and assesses the latest research trends focused on enhancing the safety and security of IoT systems through machine learning techniques. Furthermore, it investigates potential future challenges in implementing security measures within IoT systems.

In Yang et al. [21] (2022), overview of IoT equipment's physical security and safety is considered to draw attention to new research opportunities in this area. They explored various topics, including strategies for preventing theft and vandalism, as well as the design of circuits and systems, the integration of additional sensors, biometric and behavioural analysis, and tracking techniques. They provided an overview of artificial intelligence solutions aimed at enhancing the physical security and safety of IoT devices.

Mahor et al. [22] (2023) discussed several significant technologies as well as solutions to problems that citizens face as a result of a lack of digitalization. It addresses concerns such as public infrastructure, public safety, and security and provides ideal solutions. It focuses not only on AI but also on IoT, 112machine learning, deep learning, pattern reorganization, and big data analytics for the development of a smart city that is completely functional. The analysis identifies the major barriers to widespread adoption and proposes a research path to address each of them in a cost-effective manner. IoT for defense and public safety.

Rekha et al. [23] (2023) discussed the work advancement of IoT to examine every main part of IoT, and finds how some safety problems and concerns have to be recognized and discusses them momentarily. To ensure the privacy of information, it is essential to consider reliable and user-friendly IoT security that encompasses professional behaviour, integrity, encryption, intrusion detection, and the ability to identify threats, along with adaptability, interoperability, and usability. In light of certain realities, innovative IoT strategies from the scientific, educational, and industrial domains are introduced and examined by reviewing some of the current research in the IoT sector. Based on the findings of this report, it is crucial to create and implement appropriate IoT applications that can maintain integrity, security, and honesty in interconnected environments.

Souri et al. [24] (2022) provided a comprehensive analysis on the IoT communication strategies and applications for smart devices based on a systematic literature review. The communication strategies and their applications are divided into four primary categories: device-to-device, device-to-cloud, device-to-gateway, and device-to-application scenarios. Additionally, a technical taxonomy is introduced to organize existing research papers based on a search-based methodology within scientific databases. This taxonomy classifies IoT communication applications into five categories: monitoring-based communications, routing-based communications, health-based communications, intrusion-based communications, and resource-based communications. Evaluation factors and infrastructure attributes are examined through a series of technical questions.

### 1.3 Research gaps

The research gaps identified across the reviewed papers underscore several key areas where further investigation and development are warranted. Notably, existing IoT dependability frameworks often rely on informal reliability models, lacking the capability to effectively evaluate safety faults and cybersecurity threats in an integrated manner. Additionally, these frameworks struggle to address the complex interactions between co-located IoT devices and the dynamic features of self-adaptive, reconfigurable, and autonomous systems. The need for formal model-based approaches is highlighted, emphasizing the importance of accounting for safety and security interdependencies. In the context of industrial control systems, there is a recognized need for joint risk analysis frameworks, like the S-cube model-based approach, to comprehensively assess safety and security risks. Furthermore, the identified research gaps encompass the application of machine learning techniques in addressing emerging security challenges in cyber-physical systems, the enhancement of physical security measures for IoT equipment, and the development of reliable and usable IoT protection solutions to ensure integrity, security, and usability. These gaps collectively suggest a call for innovative methodologies, frameworks, and solutions to advance the robustness and resilience of IoT ecosystems across various domains.

### 1.4 Problem statement

Current IoT safety and security frameworks inadequately address the interdependencies between accidental failures and malicious attacks. Traditional methodologies analyze safety (e.g., hardware faults) and security (e.g., cyberattacks) in isolation, leading to fragmented risk assessments that overlook critical scenarios where safety faults enable security breaches, and vice versa. This gap results in incomplete mitigation strategies, leaving IoT systems vulnerable to cascading failures. To overcome this limitation, this study proposes a unified model-based framework integrating Fault Tree Analysis (FTA) and Attack Trees (AT) with Minimal Cut Sets (MCS). The framework aims to systematically identify and quantify interdependent safety-security risks, enabling holistic risk prioritization and mitigation in IoT ecosystems.

### 1.5 Objectives

The novel objectives of this study are:

1. Develop a unified model-based framework by integrating Fault Tree Analysis (FTA) and Attack Trees (AT) with Minimal Cut Sets (MCS) to jointly assess IoT safety faults and cybersecurity threats.
2. Identify and analyze the combined minimal cut sets (MCS) arising from the integrated FTA–AT framework, revealing critical interdependent fault–attack scenarios in IoT systems.
3. Quantitatively evaluate how the integrated analysis enhances IoT system resilience by characterizing and mitigating potential safety failures and security breaches.
4. Provide a systematic methodology for prioritizing and implementing targeted mitigation strategies based on insights from the unified FTA–AT–MCS analysis, improving the overall dependability of IoT deployments.

## 2. RESEARCH METHODS

### 2.1 System design

The integration of safety and security measures in IoT ecosystems is imperative, given the inherent vulnerabilities associated with both accidental failures and malicious attacks. Fault Tree Analysis (FTA) is a proven methodology for assessing safety vulnerabilities systematically. FTA involves the identification of potential failure paths within a system, mapping out the causal relationships that could lead to a safety breach. In parallel, Attack Trees (AT) provides a structured approach to evaluating the security of a system. By modeling various attack scenarios and their potential consequences, AT facilitates a comprehensive understanding of potential security risks.

Combining FTA and AT creates a unified representation that goes beyond the limitations of treating safety and security as separate entities. This integration enables a more holistic view of the interdependence between safety and security aspects within an IoT system. It acknowledges that a compromise in security can have direct implications for safety and vice versa. The intricacies of these interdependencies are often overlooked in traditional methodologies, making the unified approach crucial for a comprehensive risk assessment.

The derivation of Minimal Cut Sets is a key concept in this integrated approach. Minimal Cut Sets represent the minimal combinations of events from both safety and security analyses that could lead to identified vulnerabilities. These sets provide a clear understanding of critical paths within the system. By identifying specific components or events that, if compromised, could have cascading effects on both safety and security, the approach enables a targeted focus on areas requiring immediate attention. The Minimal Cut Sets, therefore, play a pivotal role in prioritizing mitigation strategies, ensuring a systematic and efficient response to potential risks.

This research addresses the limitations of existing approaches, where safety and security assessments are often conducted in isolation. By bridging this gap through the integration of FTA and AT with the derivation of Minimal Cut Sets, the proposed methodology aims to enhance the understanding of the risk landscape in IoT systems. The comprehensive insights gained from this integrated approach contribute to the development of a robust framework for improving the overall resilience of IoT ecosystems. The subsequent sections will delve into the detailed methodology, its practical application, and the anticipated impact of this integrated approach on the future landscape of IoT safety and security.

### 2.2 Safety and Security Challenges of the IoT System

The deployment of IoT systems introduces a myriad of safety and security challenges, reflecting the intricate landscape of interconnected devices. One primary challenge lies in the vulnerability of IoT devices to cyber threats, as the increasing number of connected devices provides a broader attack surface. Cybersecurity breaches can result in unauthorized access, data breaches, and manipulation of critical functions, posing significant risks to both the integrity and confidentiality of IoT systems. Safeguarding against sophisticated cyber threats requires a robust security framework that anticipates evolving attack vectors and ensures the resilience of the entire IoT ecosystem.

Moreover, the heterogeneity of IoT devices, encompassing a wide range of sensors, actuators, and communication protocols, introduces complexities in ensuring a unified safety and security posture. The diverse nature of these devices often leads to interoperability challenges, making it difficult to enforce consistent security measures across the entire network. Interconnected systems with varying degrees of sophistication may create weak links that adversaries can exploit. Addressing this challenge requires not only standardized security protocols but also an adaptive approach that accommodates the diversity inherent in IoT deployments.

Furthermore, the inherent constraints of IoT devices, such as limited computational power, memory, and energy resources, present unique safety and security challenges. These constraints may hinder the implementation of robust security measures, making IoT devices susceptible to resource-efficient attacks. Additionally, ensuring the safety of IoT systems involves mitigating physical risks, such as malfunctioning sensors or actuators, which can have cascading effects on the overall system functionality. Striking a balance

between efficient resource utilization and robust security measures remains a fundamental challenge in designing resilient and safe IoT systems.

The safety and security challenges of IoT systems are multifaceted, encompassing cyber threats, interoperability issues, and resource constraints. Addressing these challenges requires a holistic approach that integrates sophisticated cybersecurity measures with adaptive protocols, considering the diverse nature of IoT devices and their inherent limitations.

This paper explores how the proposed combined approach of FTA and AT, along with Minimal Cut Sets, aims to mitigate these challenges and enhance the overall safety and security of IoT ecosystems.

### 2.3 IoT Layered Model

The IoT model is structured into distinct layers, each playing a crucial role in the functioning and interconnectedness of the system. At the forefront is the Perception Layer, where sensors and actuators capture and generate data from the physical world. This layer forms the basis of IoT by collecting real-world information, enabling the system to perceive and respond to its environment. However, the Perception Layer introduces challenges related to the integrity and authenticity of the sensed data, as compromised sensor inputs can propagate inaccurate information throughout the system. Figure 1 presents the IoT four-layer architecture. The layers are the perception, network, processing, and application layer.

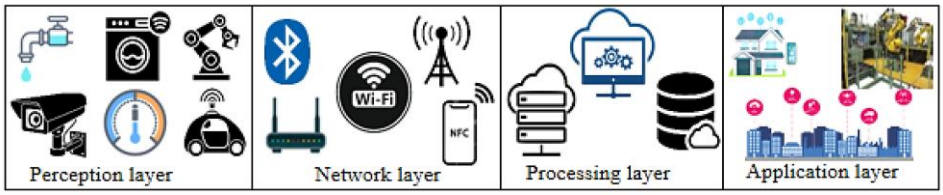


Figure 1. IoT four-layer architecture

#### 2.3.1 Perception Layer

The Perception Layer encompasses the physical devices responsible for sensing and collecting data from the environment. Sensors and actuators play a pivotal role in this layer, converting real-world events into digital signals that can be processed by the IoT system. However, the openness and ubiquity of these devices expose the system to potential security vulnerabilities. Unauthorized access to or manipulation of sensor data can lead to inaccurate perceptions, compromising the reliability and safety of the entire IoT system.

#### 2.3.2 Network Layer

The Network Layer serves as the connective tissue of the IoT model, facilitating communication and data transfer between devices. This layer introduces challenges related to data privacy and confidentiality during transmission. The sheer volume of data exchanged within the network increases the risk of eavesdropping and unauthorized access. Ensuring the security of communication channels is essential to prevent data breaches and maintain the confidentiality of sensitive information transmitted across the IoT ecosystem.

#### 2.3.3 Data Processing Layer

The Data Processing Layer is responsible for aggregating, analyzing, and interpreting the data collected from the Perception Layer. While processing this vast amount of data, challenges emerge in terms of data integrity and the potential for malicious attacks targeting algorithms and analytics engines. Ensuring the accuracy and reliability of processed data is critical for informed decision-making and preventing the propagation of erroneous information throughout the system.

#### 2.3.4 Application Layer

The Application Layer represents the interface through which end-users interact with the IoT system. Challenges in this layer often revolve around user authentication, data access controls, and the secure execution of applications. Safeguarding against unauthorized access to sensitive functionalities and ensuring the integrity of applications is vital for maintaining a secure and user-friendly IoT experience.

In essence, the layered structure of the IoT model introduces challenges at each level, ranging from the authenticity of perceived data to the secure execution of applications. Addressing these challenges necessitates a comprehensive and integrated approach that encompasses not only individual layers but also their interdependencies. This paper explores how the proposed methodology effectively tackles these challenges to enhance the safety and security of the IoT model.

### 2.4 Safety & Security Issues Across Layers

The architecture of IoT systems consists of multiple layers, each presenting its own set of safety and security challenges. This section offers a comprehensive review of safety and security research collected from various existing studies. Figure 2 illustrates a summary of the significant safety and security concerns within the layered architecture of IoT.

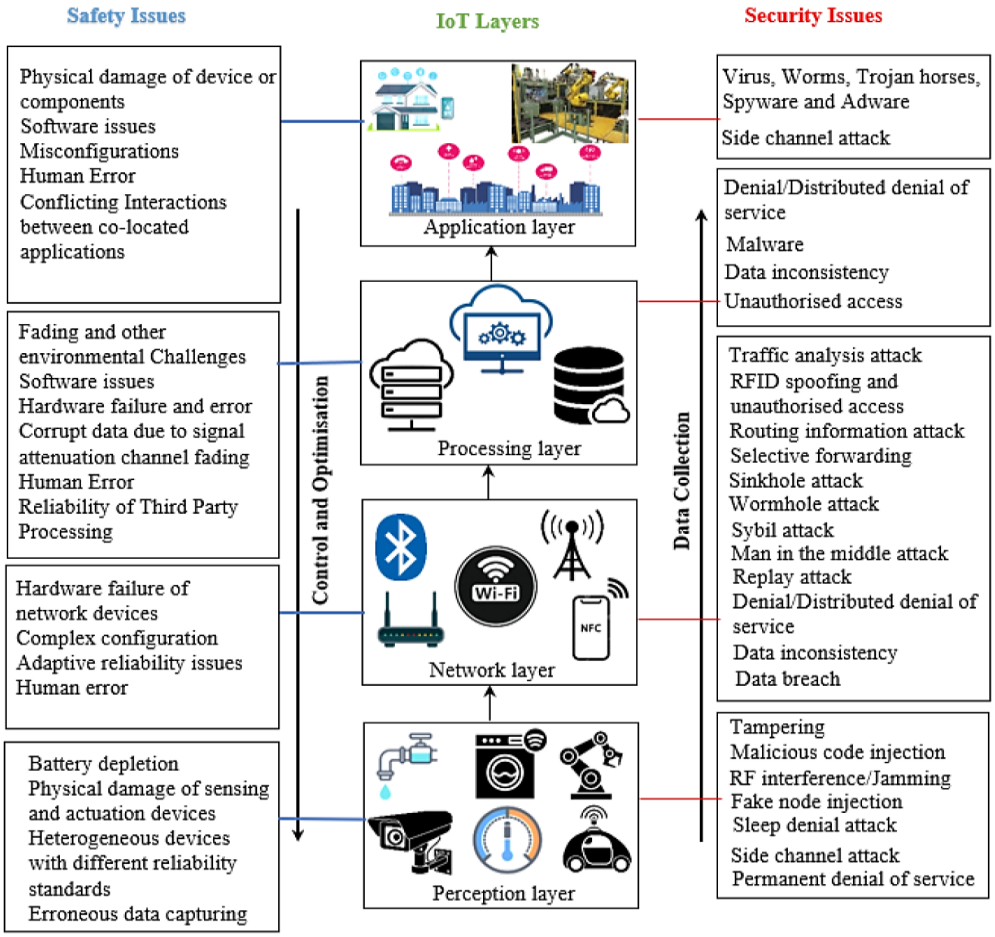


Figure 2. Safety and security issues across IoT layers

### 2.4.1 Safety and Security Issues in each layer of IoT model

A scenario to Safety and Security of IoT on remote textile boiler system is described in this section. We consider a remote textile boiler system in a garments factory in Bangladesh that implemented a smart textile boiler system shown in Figure 3 that includes Wi-Fi temperature/pressure/combustible gas sensors, Wi-Fi control electromagnetic valve, and a boiler controller.

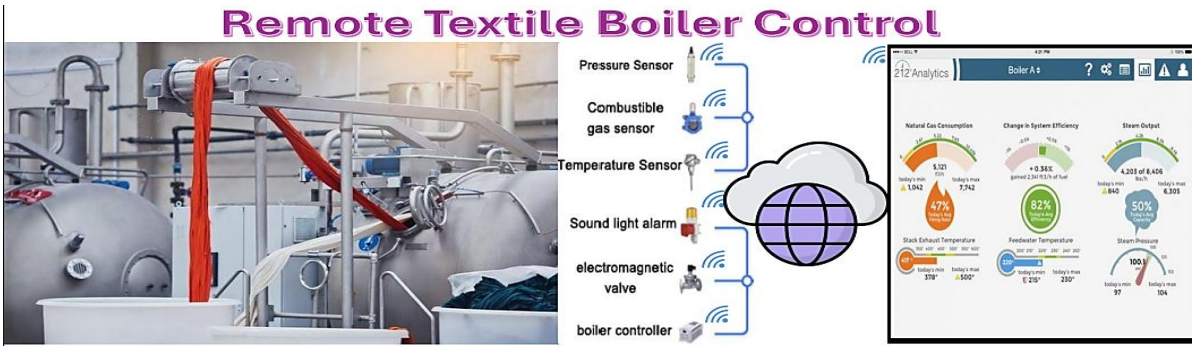


Figure 3. Remote textile boiler control system

The system is connected to the internet through a gateway (router) and integrated with Azure IoT. When the sensors detect an abnormality, the system triggers an alert in the Azure IoT management system. The management system then performs actions based on the configured settings. If equipped with AI-enabled automation, it can act according to its policy or algorithm. Otherwise, it sends an alert to the textile boiler control system to take appropriate action based on the sensor data. The boiler management team then sends commands to the boiler controller via the gateway to activate the cooler and open the pressure valve. Due to space constraints, this analysis focuses solely on the Smart Temperature Sensor (STS) component of the textile boiler

control system. The Perception Layer, comprising sensors and actuators, introduces safety and security challenges rooted in the physical collection of data. Security concerns arise from the vulnerability of these devices to tampering, unauthorized access, or physical attacks. Ensuring the integrity of sensed data is critical, as compromised sensor inputs can lead to misinformation, impacting the reliability of downstream processes.

#### 2.4.2 Perception Layer

The Perception Layer, comprising sensors and actuators, introduces safety and security challenges rooted in the physical collection of data. Security concerns arise from the vulnerability of these devices to tampering, unauthorized access, or physical attacks. Ensuring the integrity of sensed data is critical, as compromised sensor inputs can lead to misinformation, impacting the reliability of downstream processes. Safeguarding the Perception Layer involves implementing measures to detect and mitigate physical attacks on sensors and securing communication channels to prevent data manipulation.

#### 2.4.3 Network Layer

The Network Layer, responsible for facilitating communication between IoT devices, introduces multifaceted safety and security challenges. Data privacy is a paramount concern, as the transmission of sensitive information across the network may be susceptible to eavesdropping or interception. Ensuring the confidentiality and integrity of data during transit is imperative. Additionally, the proliferation of connected devices increases the attack surface, making the network vulnerable to various cyber threats. Implementing robust encryption, access controls, and intrusion detection mechanisms are crucial for fortifying the security of the Network Layer.

#### 2.4.4 Data Processing Layer

The Data Processing Layer encounters safety and security challenges during the aggregation and analysis of data. One major concern is the accuracy and reliability of processed data. Malicious actors may target algorithms and analytics engines to inject false information or manipulate outcomes, leading to incorrect insights and decisions. Moreover, privacy concerns arise as aggregated data may contain sensitive information. Protecting the integrity of data processing algorithms and implementing privacy-preserving techniques are essential for mitigating these challenges.

#### 2.4.5 Application Layer

The Application Layer, representing the interface between end-users and the IoT system, introduces safety and security challenges related to user interactions. Authentication and authorization vulnerabilities may lead to unauthorized access, posing risks to sensitive functionalities. Ensuring the secure execution of applications is vital to prevent attacks such as code injection or exploitation of software vulnerabilities. Additionally, the interconnected nature of applications may result in cascading effects if one component is compromised. Implementing strong authentication mechanisms, robust access controls, and secure coding practices are essential for fortifying the safety and security of the Application Layer.

Each layer of the IoT model presents distinct safety and security challenges, ranging from physical vulnerabilities in the Perception Layer to cybersecurity threats in the Network Layer, data integrity concerns in the Data Processing Layer, and application-level risks in the Application Layer. Addressing these challenges requires a comprehensive and integrated approach that considers the interdependencies between layers, ensuring a resilient and secure IoT ecosystem. This paper explores how the proposed combined approach of FTA and AT, along with Minimal Cut Sets, effectively address these safety and security issues across the layers of the IoT model.

### 2.5 Integration of FTA and AT

The increasing ubiquity of the IoT introduces unprecedented challenges in ensuring the safety and security of interconnected devices. This paper proposes a novel methodology that integrates Fault Tree Analysis (FTA) and Attack Trees (AT), alongside the derivation of Minimal Cut Sets, to holistically address safety and security challenges across the layers of the IoT model. The following sections delve into the key components and applications of this comprehensive methodology.

#### 2.5.1 Fault Tree Analysis

FTA serves as the foundation of the proposed methodology, providing a systematic and deductive approach to assess safety vulnerabilities within the IoT system. By initiating the analysis with the representation of the system's undesired state (top event), FTA identifies and evaluates the combination of basic component failures that could lead to this critical state. This qualitative analysis establishes Minimal Cut Sets, representing the minimal combinations of events critical to identified vulnerabilities. FTA further allows for both qualitative and quantitative analyses, empowering design engineers to ensure the safety of the proposed system.

The FTA is one of the most widely used approaches for evaluating systems' safety and reliability in different domains, including the IoT. Bell Phone Laboratories developed the approach in 1962 [24]. FTA employs a deductive method to quantify and assess the combination of fundamental component failures that might result in a top event, which are critical incidents capable of causing the entire system to fail. The process

begins with the system's unwanted condition, depicted as the top event, and methodically traces all potential routes leading to this state. Figure 4 provides a graphical representation of the FT diagram.

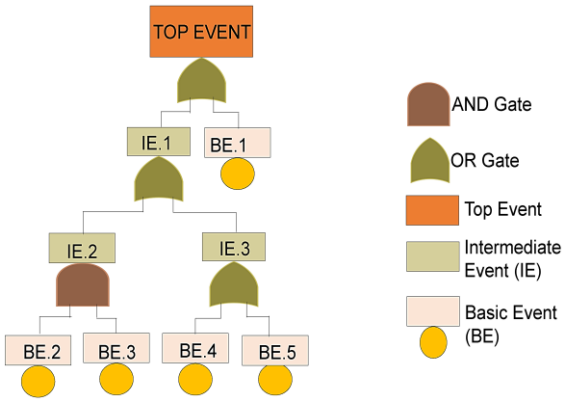


Figure 4. Fault tree framework

The primary reason for a system malfunction is identified as the top event within the Fault Tree (FT) structure. The subsequent branches and leaves of this tree are depicted as intermediate and basic events, respectively. Basic faults, shown as basic events in the tree, are interconnected using Boolean logic gates like AND and OR, depending on how these events can lead to the occurrence of subsequent events in the tree. The significance of the FT in the safety analysis of IoT systems lies in its ability to facilitate both qualitative and quantitative evaluations. These analyses, enabled by the FT framework, assist design engineers in determining the safety of a proposed system, ensuring that it meets a minimum safety threshold for safe operation and complies with the certification standards of various IoT design innovations. The qualitative analysis identifies the minimal cut sets, which encompass all the basic events for the top event. Conversely, the quantitative analysis offers probabilistic evaluations of the system's safety based on the failure probability of the basic events (components). These analyses support the iterative design process, allowing for configuration adjustments or changes in proposed components based on safety considerations.

Over the years, various extensions and modifications of the Fault Tree Analysis (FTA) have been developed in the literature. These extensions include the incorporation of additional gates to represent different fault behaviors and operating states of the systems. Notable extensions include Dynamic FT, Component FT, Pandora Temporal FT, and State/Events FT [26]. The FTA framework has been used extensively across various safety-critical domains for safety analysis. In the IoT domain, the FTA framework was used in the safety analysis of smart homes, smart grid system [27], smart aquaculture [28] and CPS, in general [28][29]. Although the studies of IoT safety design evaluation using FTA are in progress, the manual process of the approach still needs to be improved. This has been characterized as time-consuming and being performed based on cumbersome informal system models that are subject to human errors, thereby leading to inconsistency or incompleteness [26]. Another limitation of the FTA framework is that its combinatorial approach is mostly represented using the Boolean gates ‘AND’ and ‘OR’. Some of the modifications, such as the Dynamic Fault Tree and Pandora Temporal FT [30], have added such gates as the functional dependency (FDEP’), priority AND (‘PAND’) gate, and a host of others to represent the various dynamic behaviors of modern system [29]. Nevertheless, despite the relevance of the FT as one of the famous safety analysis approaches, its manual nature has left much to be desired in the analysis of IoT systems. Additionally, the basic events in the tree are assumed to be statistically independent, which, in some dynamic IoT system configurations, may not be the case [29]. These challenges suggest further research into IoT safety.

### 2.5.2 Attack Trees

Complementing FTA, Attack Trees are instrumental in modeling potential threats and security risks within the IoT system. Employing a deductive tree-like structure, as shown in Figure 5, AT illustrates various ways in which a malicious agent could compromise the system. The framework breaks down possibilities for attacks into multi-level steps, offering insights into the hierarchies of potential security breaches. By incorporating Boolean logic gates such as 'AND' and 'OR,' AT quantifies overall security metrics, enabling a comprehensive evaluation of potential attack scenarios. Leveraging AT, the methodology determines the necessary steps for malicious agents to compromise the system, aiding in informed design modifications to enhance security.

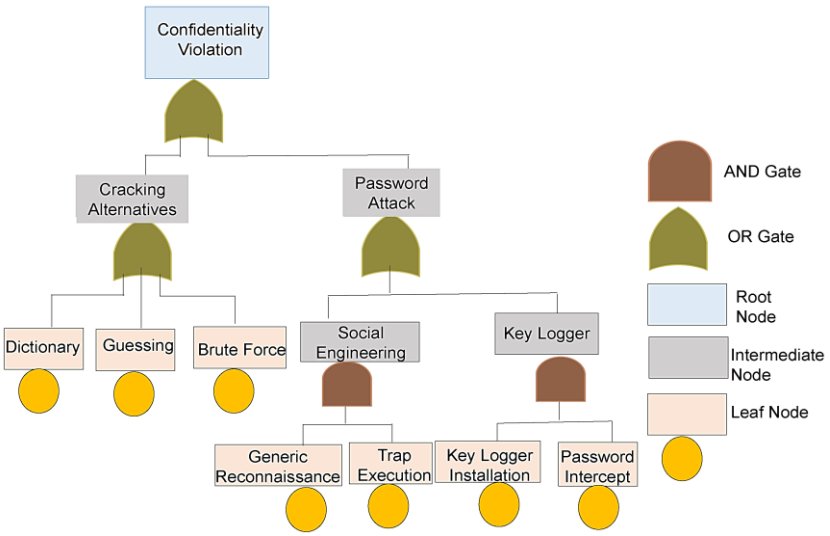


Figure 5. Attack tree example

The attack tree (AT) was developed by Schneier in 1999 to model threats against a system using a deductive tree-like structure like FTA [31]. The AT framework depicts various ways in which a system can be compromised by a malicious agent [31]. The method breaks down the potential attack scenarios for a system into multiple hierarchical levels. The various methods of compromising a system are depicted as the root, leaves, and child nodes, which intuitively represent different levels of attack hierarchies. The root node signifies the attacker's ultimate objective. The nodes lower in the hierarchy refine the goals of the root node, detailing basic actions the attacker must undertake to reach their primary objective [32][33]. Dependencies among nodes at the same hierarchical level are modelled using Boolean 'AND' and 'OR' gates. In 'AND' scenarios, all specified goals must be met to compromise the parent node, whereas in 'OR' scenarios, achieving any one of the goals suffices. Quantitatively, the system's overall security metrics can be derived from the values of the child nodes and their respective Boolean logic conditions. Refer to the example attack tree shown in Fig 4. This tree deductively demonstrates how cyber-security threats can be orchestrated to compromise one of the system's CIA triads, ultimately affecting the IoT system's reliability. The framework outlines the sequential steps malicious agents must take to exploit various vulnerabilities before breaching the confidentiality of IoT data. Additionally, subjective quantitative metrics can be incorporated at each step using known techniques like fuzzy logic and vulnerability quantification. This approach aids security engineers in assessing and prioritizing security designs to create secure and reliable systems.

### 2.5.3 Minimal Cut Sets

The derivation of Minimal Cut Sets plays a pivotal role in bridging insights gained from FTA and AT. These sets represent minimal combinations of events critical to identified vulnerabilities, providing a targeted focus on specific components or events crucial to the overall safety and security of the IoT system. Integration of FTA and AT findings through Minimal Cut Sets facilitates a nuanced understanding of intricate interdependencies between safety and security aspects, enabling a more effective risk mitigation strategy.

Minimal Cut Sets are sets of events or conditions whose simultaneous occurrence is sufficient to cause a specific undesired outcome or failure in the system. In the context of safety and security analysis, these sets represent the minimal combinations of faults (from FTA) and attacks (from AT) that could lead to identified vulnerabilities in the IoT system.

### 2.5.4 Mathematical Representation

Let's denote the events or conditions in the system as:

$$E_1, E_2, \ldots . E_n \quad (1)$$

where, $n$ is the total number of events considered in the safety and security analysis. The Minimal Cut Sets can be represented as sets of these events.

$$MCS_1 = \{E_{i1}, E_{i2}, \ldots\ldots, E_{ik}\}$$
$$MCS_2 = \{E_{ij}, E_{j2}, \ldots\ldots, E_{jm}\}$$
$$\vdots$$
$$MCS_p = \{E_{l1}, E_{l2}, \ldots\ldots, E_{lq}\} \quad (2)$$

where, $p$ is the total number of Minimal Cut Sets identified. Each Minimal Cut Set $MCS_i$ consists of specific events $E_{ix}$ that, if they occur simultaneously, can lead to the undesired outcome.

2.5.5 Application in Risk Mitigation

The identification of Minimal Cut Sets is crucial for focusing risk mitigation strategies on specific components or events. By understanding these minimal combinations, design engineers can prioritize their efforts in addressing the most critical aspects of safety and security.

2.5.6 Example Scenario

Let's consider an example where $E_1$ represents a hardware failure identified in FTA, and $E_2$ represents a specific cyber-attack identified in AT. A Minimal Cut Set$MCS_1 = \{E_1, E_2\}$ indicates that both the hardware failure and the cyber-attack need to occur simultaneously for a particular safety or security vulnerability to manifest.

2.5.7 Equation for Integration

The integration of FTA and AT findings through Minimal Cut Sets can be expressed as follows:

$$IntegratedRisk = \sum_{i=1}^{p} Weight(MCS_i) \quad (3)$$

where, $Weight(MCS_i)$ represents the weight assigned to each Minimal Cut Set based on the severity or criticality of the events included. This integrated risk metric provides a comprehensive assessment of the safety and security aspects, considering the nuanced interdependencies identified through Minimal Cut Sets.

In summary, Minimal Cut Sets provide a systematic way to identify and prioritize the critical combinations of faults and attacks in an IoT system, aiding in the development of effective risk mitigation strategies.

2.5.8 Holistic IoT Model Approach

The proposed methodology is applied comprehensively across the layers of the IoT model, addressing specific challenges and risks associated with the Perception Layer, Network Layer, Data Processing Layer, and Application Layer. Systematically analyzing safety and security issues at each layer provides a comprehensive overview of potential vulnerabilities and threats, ensuring the resilience of the entire IoT ecosystem against both accidental and intentional risks.

2.5.9 Algorithm for Integrated Analysis

The algorithm for integrated safety and security analysis for IoT can be shown in Algorithm 1.

Algorithm 1: Integrated Safety and Security Analysis for IoT

Input : System Components (C), Attack Scenarios (A), Failure Modes (F)
Output : Integrated Minimal Cut Sets (IMCS)

1. Initialize sets:
   - Safety Minimal Cut Sets (SMCS) = ∅
   - Security Minimal Cut Sets (SeMCS) = ∅
   - Integrated Minimal Cut Sets (IMCS) = ∅
2. **Safety Analysis**. Perform Fault Tree Analysis (FTA) for each failure mode in F:
   - Identify Basic Events (BE) using formalized system model equations.
   - Determine Safety Minimal Cut Sets (SMCS) for each failure mode.
3. **Security Analysis**. Perform Attack Trees (AT) analysis for each attack scenario in A:
   - Identify Attack Steps (AS) using system vulnerabilities.
   - Determine Security Minimal Cut Sets (SeMCS) for each attack scenario.
4. **Integration**. Combine SMCS and SeMCS to obtain IMCS: IMCS = SMCS ∪ SeMCS
5. **Risk Mitigation**. For each IMCS:
   - Assess risk severity and criticality using predefined metrics.
   - Develop targeted risk mitigation strategies based on IMCS.
6. Return IMCS

End Algorithm

The combined approach of FTA and AT, enriched by the derivation of Minimal Cut Sets, constitutes a robust methodology to effectively address safety and security challenges in the IoT model. This holistic approach aims to enhance the overall resilience of IoT systems, providing actionable insights for design engineers to implement effective risk mitigation strategies in the evolving landscape of IoT safety and security.

## 3. RESULTS AND DISCUSSION

### 3.1 Dataset Description

We utilized a comprehensive IoT dataset collected from [34]. The dataset comprises data from various sensors, devices, and communication networks in a real-world IoT environment. Table 1 provides an overview of the key attributes and statistics of the dataset. This is IoT dataset for Intrusion Detection Systems (IDS). BoTNeTIoT-L01 is a dataset that consolidates all IoT device data files from the

detection_of_IoT_botnet_attacks_N_BaIoT (BoTNeTIoT) dataset [34]. This updated version minimizes redundancy by selecting features within a 10-second time window. In the dataset, the class label 0 indicates attacks, while 1 represents normal samples.

The BoTNeTIoT-L01, the most recent dataset, contains nine IoT devices traffic sniffed using Wireshark in a local network using a central switch. It includes two Botnet attacks (Mirai and Gafgyt). The dataset contains twenty-three statistically engineered features extracted from the .pcap files. Statistical measures were computed (mean, variance) over the time window of 10 sec with decay factor equals 0.1.

Table 1. BoTNeTIoT-L01 dataset description

| Attribute | Description |
|---|---|
| Dataset Name | BoTNeTIoT-L01 |
| Reduction of Redundancy | Selected features from a 10-second time window only |
| Class Label | 0: Attacks, 1: Normal Samples |
| Devices Sniffed | Nine IoT devices |
| Botnet Attacks | Mirai, Gafgyt |
| Features | Twenty-three statistically engineered features |
| Time Window | 10 seconds |
| Decay Factor | 0.1 |

In this paper, we test only for Gafgyt and Mirai attacks in exploiting vulnerabilities and compromising IoT devices, whereas phishing and malware spoofing attacks typically target different aspects of cybersecurity, such as user interactions and software vulnerabilities.

#### 3.1.1 Gafgyt Attack in IoT

Gafgyt, also known as BASHLITE or Lizkebab, is a type of malware that targets IoT devices. This malicious software is designed to infect and compromise vulnerable devices, turning them into bots within a larger botnet. Gafgyt primarily exploits weak security credentials and vulnerabilities in IoT devices, often using brute-force attacks to gain unauthorized access. Once a device is compromised, it can be used for various malicious activities, such as launching distributed denial-of-service (DDoS) attacks, spreading malware, or participating in other forms of cybercrime. The impact of a Gafgyt attack on IoT devices can range from disrupting normal device functionality to contributing to large-scale network-based attacks.

#### 3.1.2 Mirai Attack in IoT

Mirai gained notoriety for its role in orchestrating massive DDoS attacks by leveraging compromised IoT devices. Similar to Gafgyt, Mirai targets devices with weak security, often exploiting default usernames and passwords. Once a device is infected, it becomes part of the Mirai botnet, which can be controlled remotely to carry out coordinated attacks. Mirai has been responsible for some of the largest DDoS attacks recorded, disrupting online services and causing widespread network outages. The attack's impact extends beyond individual device compromise, posing significant challenges in securing and managing IoT ecosystems due to the sheer scale and sophistication of Mirai-based attacks.

### 3.2 Analysis and Findings

#### 3.2.1 Metrics

a. Risk severity

Risk severity refers to the potential impact or consequences of a specific risk or hazard if it were to materialize. It assesses the seriousness of the harm or damage that could result from an adverse event.

$$Risk\ Severity = Safety\_Probability * Security\_Probability \quad (4)$$

b. Risk Priority

Risk priority, also known as risk priority number (RPN) or risk priority index (RPI), is a quantitative measure used to prioritize risks based on their severity, probability, and detectability. It helps in determining which risks should be addressed first.

$$Risk\ Priority = Safety\_Probability + Security\_Probability \quad (5)$$

#### 3.2.2 Statistical metrics

Statistical metrics include the mean and variance. $Mean = (Sum\ of\ all\ values) / (Number\ of\ values)$. $Variance = \Sigma\ [(x - \mu)^2] / n$, where $\mu$ is the mean

### 3.3 Safety & Security Assessment Results

In our proposed system is tested in recent BoTNeTIoT-L01 dataset for safety and security probability.

$\boldsymbol{mean} = 31(0.005+0.002+0.008) = 0.005.$

$\boldsymbol{variance^2} = \frac{1}{3}\ [(0.005\text{-}0.005)^2 + (0.002\text{-}0.005)^2 + (0.008\text{-}0.005)^2] = \mathbf{0.000006}$

In Table 2, the integrated safety and security assessment for IoT provides a comprehensive overview of various fault scenarios and associated attack vectors. The Safety_Probability column quantifies the likelihood of safety-related faults, while the Security_Probability column indicates the probability of security-related attacks. For instance, Fault_ID 1 (Data_Corruption) with a Safety_Probability of 0.005 is linked to Attack_ID 101 (Mirai) with a Security_Probability of 0.01. Similarly, other fault scenarios like Device_Failure and Communication_Interruption are associated with specific attack vectors (Gafgyt and Mirai, respectively) along with corresponding probabilities. This integrated table offers valuable insights into potential risks and their interconnectedness within the IoT system.

Table 2. Integrated Safety and Security Assessment for IoT

| Fault_ID | Fault_Name | Safety_Probability | Attack_ID | Attack_Name | Security_Probability |
|---|---|---|---|---|---|
| 1 | Data_Corruption | 0.005 | 101 | Mirai attack | 0.010 |
| 2 | Device_Failure | 0.002 | 102 | Gafgyt attack | 0.015 |
| 3 | Communication_Interruption | 0.008 | 103 | Mirai attack | 0.008 |
| | Statistical measure | **Value** | | | |
| | $mean\ (\mu)$ | 0.005 | | | |
| | $var\,i\,ance^2$ | 0.000006 | | | |

The comprehensive safety and security assessment conducted on the IoT system using the BoTNeTIoT-L01 dataset revealed significant findings. Three primary fault scenarios, including data corruption, device failure, and communication interruption, were identified with corresponding safety probabilities of 0.005, 0.002, and 0.008, respectively. Security vulnerabilities were assessed through attack scenarios, focusing on Mirai and Gafgyt attacks, with security probabilities of 0.01 and 0.015, respectively.

The calculated statistical measures, indicating 0.005 for safety and 0.000006 for security, offer a quantitative representation of the system's safety and security status. This integrated assessment facilitates a holistic understanding of the interdependence between safety and security aspects, leading to the identification of common findings and minimal cut sets for targeted risk mitigation.

These findings emphasize the significance of adopting an integrated approach to address safety and security challenges in IoT systems. The discussion surrounding these results contributes to the ongoing discourse on fortifying the resilience of IoT systems, highlighting the necessity for adaptive strategies to counter evolving safety and security challenges in the dynamic landscape of the Internet of Things. The combined insights from safety and security assessments enable design engineers to implement effective risk mitigation strategies, ensuring the robustness and reliability of IoT systems in the face of potential threats and vulnerabilities. As the IoT ecosystem continues to evolve, this integrated approach becomes crucial for staying ahead of emerging risks and adapting security measures to safeguard the interconnected devices and networks.

### 3.4 Discussion

#### 3.4.1 Implications of Minimal Cut Sets for IoT Risk Management

Our integrated FTA–attack-tree methodology uses minimal cut sets (MCS) to identify the smallest combinations of component failures and attack steps that cause a system-level failure. In traditional FTA, an MCS is defined as the minimal set of basic events leading to the top event. By extending this to include attacker actions, each MCS in our combined model can mix safety failures (like sensor faults or power loss) with security breaches (such as an exploited vulnerability). This highlights how certain faults and attacks interact: for example, an attacker taking control of a sensor and a coinciding power outage might together trigger a dangerous IoT system failure. Identifying these mixed MCS makes clear which combinations of safety and security risks are most critical. In practical terms, risk managers can focus on breaking up those critical combinations – perhaps by hardening a component that appears in many MCS or by adding redundancy for a vulnerable function. Thus, MCS serve as a lens to see exactly how a safety issue and a security issue can reinforce each other. This focused insight helps prioritize mitigation resources on the points in the system that contribute to the highest-risk cut sets, making IoT risk management both more targeted and effective.

#### 3.4.2 Revealing Safety-Security Interdependencies

The MCS-based integration also reveals hidden interdependencies between safety and security events. In a purely safety-focused analysis, one might list sensor failures or hardware faults in isolation; similarly, a security analysis might list possible attack paths independently. In our combined model, minimal cut sets can contain both types of events. For example, an MCS might include a “software exploit” basic event together with a “sensor degradation” failure. This explicitly shows that the sensor’s degradation and the exploit together cause the top-level hazard – indicating a security attack is exacerbating a safety vulnerability. Such examples make it clear when a security breach directly leads to a safety incident, or vice versa. By exposing these mixed scenarios, system designers can see how a safety mechanism (like a critical sensor) could become a security vulnerability if an attacker can sabotage it. Conversely, they can see how a defensive security measure (e.g. an encrypted control message) might fail to prevent a certain cascading failure unless paired with a hardware fix.

Understanding these links means mitigation can be cross-disciplinary: teams can devise countermeasures that address both domains. For instance, if a particular MCS shows that a particular device failure enables an attack, then improving that device's reliability also strengthens security. Overall, mapping out these interdependencies through MCS enables more resilient designs by ensuring that safety and security are not treated as separate silos but as deeply connected aspects of IoT system behavior.

### 3.4.3 Comparison with Prior Studies

Abdulhamid et al. (2024) studied the reliability of an IoT Smart Irrigation System using FTA [17]. They proposed a security-based model (MBSA) for failures, but their work focused on identifying failure paths (safety faults) rather than modeling actual attacks. In contrast, our study overlays attack trees on the fault tree and computes MCS that combine failures and attacks. This means we capture scenarios that neither approach alone would reveal, advancing beyond their purely safety-driven FTA analysis.

Kriaa et al. (2015–2019) surveyed methods for joint safety-security analysis (largely in industrial control systems) [18]. Their work raised awareness of safety–security convergence and discussed conceptual interactions, but it was more theoretical and ICS-oriented. By comparison, we apply a concrete integrated model to IoT, using actual fault and attack trees to quantify interdependencies. Unlike Kriaa et al., our approach directly computes minimal cut sets in an IoT context, providing actionable risk rankings rather than just high-level survey insights.

Ihirwe et al. (2023) focus on safety analysis by using testing to refine failure logic in IoT (Failure Logic Analysis) [19]. They enhance safety models with testing to improve completeness, but they do not consider cyber-attacks. Our study goes further by incorporating security events into the safety analysis. In other words, while their method helps predict failure scenarios through tests, it only addresses component faults. We extend the analysis to include attacker-induced faults, thereby filling the gap they leave by combining both sources of hazard in one model.

Abbas et al. (2018) (Ahmed et al., 2018) conducted a literature review on malicious insider attacks in IoT healthcare systems [20]. They identified various attack scenarios and risks but did not model how those attacks interact with system failures. Our work builds on the idea of security threats in IoT but goes beyond a review by embedding those threats into a fault-tree framework. This allows us to quantify how an insider attack could, for example, lead to a loss of medical equipment safety. Thus, we transform descriptive insights from Abbas et al. into concrete minimal cut sets that guide mitigation.

Yang et al. (Year) examined IoT security risks using attack-tree methods [21]. Their approach catalogued attack paths and evaluated their probabilities, but it considered security in isolation. We extend such security-focused analysis by merging it with fault tree analysis. In practice, this means we take the attack scenarios Yang et al. identified and see how they combine with failures. This integration reveals, for instance, that some attacks are only critical because of coincident system faults.

Mahor et al. (2022) proposed a blockchain-based framework to enhance IoT security (e.g. detecting anomalies or ensuring data integrity) [22]. Their solution improves security monitoring but treats failures and attacks separately. In contrast, our integrated cut-set method uses such security insights as inputs but then relates them to potential system failures. In other words, while Mahor et al. strengthen one part of the system, we quantify how that part's compromise could affect overall safety.

Rekha et al. (2021) provided a broad survey of IoT security issues and solutions. This work compiled common threats and defenses (e.g. encryption, authentication) but did not perform modeling or quantitative analysis [23]. Our study takes those general findings and embeds them into a unified model. Instead of only listing solutions, we show which combinations of the surveyed threats and system faults are most dangerous, thus giving more precise guidance than a general survey.

Souri et al. (2024) presented a cloud-based cyber-attack detection architecture for industrial IoT [24]. Their system can identify malicious behaviors, but it does not analyze how those attacks connect to safety outcomes. By contrast, our approach can take an attack like the ones Souri et al. detect and immediately see its impact on system safety via the cut sets. This closes the loop by linking security monitoring results back to safety risk – an advancement beyond pure detection.

### 3.4.4 Contributions to Future IoT Resilience

By exposing the linked safety–security hazards via minimal cut sets, this work equips engineers with a concrete roadmap for resilience. Rather than fixing problems one at a time, they can now target the worst-case combinations. For example, if an MCS shows that a certain network intrusion together with a specific component failure causes system collapse, then strengthening either the network security or the component's reliability (or both) will effectively break that cut set. This dual insight leads to defense-in-depth strategies that cover both domains simultaneously. In future IoT designs, embedding this combined analysis means that adding new security features will be done with awareness of safety, and safety measures will be chosen with security in mind. In sum, our study provides a structured way to co-design safety and security: it identifies the "weakest links" that bridge both, so that fixing them yields a more robust IoT system overall. This integrated perspective –

grounded in minimal cut sets – thus contributes to building smarter mitigation strategies and ultimately to more trustworthy, resilient IoT deployments.

## 4. CONCLUSION

This work addressed the stated problem by delivering a unified FTA–AT–MCS framework for IoT dependability analysis. When applied to a representative IoT dataset (BoTNeTIoT-L01), the methodology identified concrete correlations between safety faults and security attacks, revealing minimal cut sets that span both domains. For example, faults like Data_Corruption were found to be associated with attacks such as Mirai, illustrating how the combined analysis uncovers vulnerabilities across safety and security. These findings confirm that the integrated approach quantitatively captures interdependent failure and attack scenarios that isolated analyses would miss. By pinpointing these critical event combinations, the framework enables targeted mitigation of the most impactful risks. Thus, the proposed solution directly fulfills the research objective by providing a comprehensive, model-based safety–security assessment for IoT systems. In summary, the integrated FTA–AT methodology with minimal cut sets successfully bridges the gap identified in the problem statement, providing actionable insights for enhancing IoT robustness. Future work will further refine this approach by incorporating real-time threat detection and pursuing standardization efforts to address evolving IoT challenges.

## REFERENCE

[1] C. de Villiers, S. Kuruppu, dan D. Dissanayake, "A (New) Role for Business–Promoting the United Nations' Sustainable Development Goals through the Internet-of-Things and Blockchain Technology," *J. Bus. Res*., vol. 131, pp. 598–609, 2021. https://doi.org/10.1016/j.jbusres.2020.11.066

[2] Z. Allam, S. E. Bibri, D. S. Jones, D. Chabaud, dan C. Moreno, "Unpacking the '15-Minute City' via 6G, IoT, and Digital Twins: Towards a New Narrative for Increasing Urban Efficiency, Resilience, and Sustainability," *Sensors*, vol. 22, no. 4, art. 1369, Feb. 2022. https://doi.org/10.3390/s22041369

[3] T. Katika, F. K. Konstantinidis, T. Papaioannou, A. Dadoukis, S. N. Boleirakis, G. Tsimiklis, dan A. Amditis, "Exploiting Mixed Reality in a Next-Generation IoT Ecosystem of a Construction Site," in *Proc. IEEE Int. Conf. Imaging Syst. and Techniques* (*IST*), 2022, pp. 1–6. https://doi.org/10.1109/IST55454.2022.9827726

[4] M. Mobasshir, "IoT Ecosystem: Functioning Framework, Hierarchy of Knowledge, and Intelligence," in *Artificial Intelligence-Based Internet of Things Systems*, 2022, pp. 47–76. https://doi.org/10.1007/978-3-030-87059-1_2

[5] Y. Wu, HN. Dai, H. Wang, Z. Xiong, S. Guo, "A Survey of Intelligent Network Slicing Management for Industrial IoT: Integrated Approaches for Smart Transportation, Smart Energy, and Smart Factory," *IEEE Commun. Surveys Tuts*., vol. 24, no. 2, pp. 1175–1211, 2022. https://doi.org/10.1109/COMST.2022.3158270

[6] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, dan H. Arshad, "The Internet of Things Security: A Survey Encompassing Unexplored Areas and New Insights," *Comput. & Security*, vol. 112, art. 102494, 2022. https://doi.org/10.1016/j.cose.2021.102494

[7] A. M. Ashraf, W. Imran, dan L. Vechot, "Analysis of the Impact of a Pandemic on the Control of the Process Safety Risk in Major Hazards Industries Using a Fault Tree Analysis Approach," *J. Loss Prevent. Process Ind*., vol. 74, art. 104649, 2022. https://doi.org/10.1016/j.jlp.2021.104649

[8] S. U. R. Malik, A. Anjum, S. A. Moqurrab, dan G. Srivastava, "Towards Enhanced Threat Modelling and Analysis Using a Markov Decision Process," *Comput. Commun*., vol. 194, pp. 282–291, 2022. https://doi.org/10.1016/j.comcom.2022.07.038

[9] R. Maciel, J. Araujo, C. Melo, P. Pereira, J. Dantas, dan P. Maciel, "Impact Evaluation of DDoS and Malware Attack Using IoT Devices," in *Distributed Denial of Service Attacks: Concepts, Mathematical and Cryptographic Solutions*, vol. 6, 2021, p. 1. https://doi.org/10.1515/9783110619751-001

[10] F. O. Ehiagwina, O. O. Kehinde, A. S. Nafiu, L. O. Afolabi, dan I. S. Olatinwo, "Fault Tree Analysis and its Modifications as Tools for Reliability and Risk Analysis of Engineering Systems–An Overview," *Int. J. Res. Publ. Rev*., vol. 3, no. 1, pp 383-396, 2025.

[11] A. Wieland, "Dancing the Supply Chain: Toward Transformative Supply Chain Management," *J. Supply Chain Manag*., vol. 57, no. 1, pp. 58–73, 2021. https://doi.org/10.1111/jscm.12209

[12] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu, I. Kevin, dan K. Wang, "Hierarchical Adversarial Attacks Against Graph-Neural-Network-Based IoT Network Intrusion Detection System," *IEEE Internet Things J*., vol. 9, no. 12, pp. 9310–9319, 2021. https://doi.org/10.1109/JIOT.2021.3130434

[13] T. A. Ahanger, A. Aljumah, dan M. Atiquzzaman, "State-of-the-Art Survey of Artificial Intelligent Techniques for IoT Security," *Comput. Netw*., vol. 206, art. 108771, 2022. https://doi.org/10.1016/j.comnet.2022.108771

[14] B. Ghimire dan D. B. Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8229–8249, 2022. https://doi.org/10.1109/JIOT.2022.3150363
[15] A. T. Atieh, "Establishing Efficient IT Operations Management through Efficient Monitoring, Process Optimization, and Effective IT Policies," *Empirical Quests Manag. Essences*, vol. 1, no. 1, pp. 1–12, 2021.
[16] A. Corallo, M. Lazoi, M. Lezzi, dan P. Pontrandolfo, "Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level," *IEEE Trans. Eng. Manag.*, vol. 70, no. 11, pp. 3745–3765, 2023. https://doi.org/10.1109/TEM.2021.3084687
[17] A. Abdulhamid, S. Kabir, I. Ghafir, dan C. Lei, "Dependability of the Internet of Things: Current Status and Challenges," in *Proc. 2022 Int. Conf. Electr., Comput., Commun. and Mechatronics Eng.* (*ICECCME*), 2022, pp. 1–6. https://doi.org/10.1109/ICECCME55909.2022.9987845
[18] S. Kriaa, M. Bouissou, dan Y. Laarouchi, "A New Safety and Security Risk Analysis Framework for Industrial Control Systems," *Proc. Inst. Mech. Eng., Part O: J. Risk Reliab.*, vol. 233, no. 2, pp. 151–174, 2019. https://doi.org/10.1177/1748006X18765885
[19] F. Ihirwe, D. Di Ruscio, K. Di Blasio, S. Gianfranceschi, dan A. Pierantonio, "Supporting Model-Based Safety Analysis for Safety-Critical IoT Systems," *J. Comput. Lang.*, art. 101243, 2023. https://doi.org/10.1016/j.cola.2023.101243
[20] G. Abbas, A. Mehmood, M. Carsten, G. Epiphaniou, dan J. Lloret, "Safety, Security and Privacy in Machine Learning Based Internet of Things," *J. Sensor Actuator Netw.*, vol. 11, no. 3, art. 38, 2022. https://doi.org/10.3390/jsan11030038
[21] X. Yang, L. Shu, Y. Liu, G. P. Hancke, M. A. Ferrag, dan K. Huang, "Physical Security and Safety of IoT Equipment: A Survey of Recent Advances and Opportunities," *IEEE Trans. Ind. Inform.*, vol. 18, no. 7, pp. 4319–4330, 2022. https://doi.org/10.1109/TII.2022.3141408
[22] V. Mahor, R. Rawat, A. Kumar, B. Garg, dan K. Pachlasiya, "IoT and Artificial Intelligence Techniques for Public Safety and Security," in *Smart Urban Computing Applications, River Publishers*, 2023, pp. 111–126.
[23] S. Rekha, L. T. Thirupathi, S. Renikunta, dan R. Gangula, "Study of Security Issues and Solutions in Internet of Things (IoT)," *Mater. Today: Proc.*, vol. 80, pp. 3554–3559, 2023. https://doi.org/10.1016/j.matpr.2021.07.295
[24] A. Souri, A. Hussien, M. Hoseyninezhad, dan M. Norouzi, "A Systematic Review of IoT Communication Strategies for an Efficient Smart Environment," *Trans. Emerg. Telecommun. Tech.*, vol. 33, no. 3, e3736, 2022. https://doi.org/10.1002/ett.3736
[25] S. Bhattacharyya dan A. Cheliyan, "Optimization of a Subse a Production System for Cost and Reliability Using Its Fault Tree Model," *Reliab. Eng. Syst. Saf.*, vol. 185, pp. 213–219, 2019. https://doi.org/10.1016/j.ress.2018.12.030
[26] K. Aslansefat, S. Kabir, Y. Gheraibia, dan Y. Papadopoulos, "Dynamic Fault Tree Analysis: State-of-the-Art in Modeling, Analysis, and Tools," in *Reliability Management and Engineering*, CRC Press, 2020, pp. 73–112.
[27] M. Bilgen dan N. Altin, "An Overview on Reliability Analysis and Evaluation Methods Applied to Smart Grids," *Gazi Univ. J. Sci. Part C Des. Technol.*, vol. 9, pp. 645–660, 2021.
[28] P. Niloofar dan S. Lazarova-Molnar, "Fusion of Data and Expert Knowledge for Fault Tree Reliability Analysis of Cyber-Physical Systems," in *Proc. 2021 5th Int. Conf. System Reliability and Safety* (*ICSRS*), Palermo, Italy, 24–26 Nov. 2021, pp. 92–97.
[29] A. A. Musa, A. Hussaini, W. Liao, F. Liang, dan W. Yu, "Deep Neural Networks for Spatial-Temporal Cyber-Physical Systems: A Survey," *Future Internet*, vol. 15, art. 199, 2023. https://doi.org/10.3390/fi15060199
[30] S. Kabir, "A Fuzzy Data-Driven Reliability Analysis for Risk Assessment and Decision Making Using Temporal Fault Trees," *Decis. Anal. J.*, vol. 8, art. 100265, 2023. https://doi.org/10.1016/j.dajour.2023.100265
[31] D. M. Gabbay, R. Horne, S. Mauw, dan L. van der Torre, "Attack-Defence Frameworks: Argumentation-Based Semantics for Attack-Defence Trees," in *Graphical Models for Security: 7th Int. Workshop*, GraMSec 2020, Boston, MA, USA, 22 June 2020, pp. 143–165.
[32] P. J. Brooke dan R. F. Paige, "Fault Trees for Security System Design and Analysis," *Comput. Secur.*, vol. 22, pp. 256–264, 2003. https://doi.org/10.1016/S0167-4048(03)00313-4
[33] Neha dan A. Maurya, "Cyber Attack Modeling Recent Approaches: A Review," in *Proc. 3rd Int. Conf. Computing, Communications, and Cyber-Security*, Virtual, 26–28 May 2023, pp. 871–882.
[34] Alaa Alhowaide, "IoT Data Set," Kaggle, 14 Mar. 2025. [Online]. Available: https://www.kaggle.com/datasets/azalhowaide/iot-dataset-for-intrusion-detection-systems-ids