Informatics in Education, 2023, Vol. 22, No. 4, 555–588

DOI: 10.15388/infedu.2023.30

IoT Security Risk Management: A Framework and Teaching Approach

Abasi-amefon O. AFFIA[1], Alexander NOLTE[1,2], Raimundas MATULEVIČIUS[1]

[1]*University of Tartu, Tartu, Estonia*
[2]*Carnegie Mellon University, Pittsburgh, USA*
e-mail: amefon.affia@ut.ee, alexander.nolte@ut.ee, rma@ut.ee

Received: December 2022

Abstract. While Internet of Things (IoT) devices have increased in popularity and usage, their users have become more susceptible to cyber-attacks, thus emphasizing the need to manage the resulting security risks. However, existing works reveal research gaps in IoT security risk management frameworks where the IoT architecture – building blocks of the system – are not adequately considered for analysis. Also, security risk management includes complex tasks requiring appropriate training and teaching methods to be applied effectively. To address these points, we first proposed a security risk management framework that captures the IoT architecture perspective as an input to further security risk management activities. We then proposed a hackathon learning model as a practical approach to teach hackathon participants to apply the IoT security risk management framework. To evaluate the benefits of the framework and the hackathon learning model, we conducted an action research study that integrated the hackathon learning model into a cybersecurity course, where students learn how to apply the framework. Our findings show that the IoTA-SRM framework was beneficial in guiding students towards IoT security risk management and producing repeatable outcomes. Additionally, the study demonstrated the applicability of the hackathon model and its interventions in supporting the learning of IoT security risk management and applying the proposed framework to real-world scenarios.

Keywords: Internet of Things (IoT), security risk management, hackathons, security learning.

1. Introduction

The Internet of Things (IoT) has revolutionized how we live and work, connecting billions of objects to the Internet to gather, process, store, distribute, and use data. Critical domains such as healthcare, transportation, and emergency services rely heavily on IoT systems (Resul and Gündüz, 2020). However, IoT systems are vulnerable to cyber-attacks, which can have catastrophic consequences on human lives (Fries *et al.*, 2009). Therefore, securing IoT systems from security vulnerabilities is crucial. Previous

research has highlighted the importance of considering the IoT system architecture in security assessment (Cvitić *et al.*, 2015; Huang *et al.*, 2016; Malik and Singh, 2019).

However, these approaches do not consider the architecture perspective as an input to security risk management. Nonetheless, research gaps result from an uneven focus on certain IoT architecture layers for risk management instead of a more comprehensive analysis. Thus, the principles of security by design are not fully realized. In this context, we explore the research question:

RQ1. *How can the IoT architecture perspective be incorporated into existing security risk management methods for IoT systems?*

To address **RQ1**, we propose an IoT architecture-based Security Risk Management (IoTA-SRM) framework that incorporates the IoT architecture perspective into security risk management methods for IoT systems. By considering the IoT architecture as an input to the security risk management process, our proposed framework can help stakeholders ensure that relevant assets and relationships are identified and accounted for; and that the security risks are properly analyzed and mitigated.

However, studies have shown a disconnect between theory and practice in current strategies for educating cybersecurity professionals (Kessler, 2012) on securing critical systems. As a result, security frameworks may encounter challenges in their practical implementation due to the expertise and knowledge required to execute them effectively. This gap between theory and practice can reduce the chances of successfully implementing the framework in actual IoT systems, making it difficult to protect them in an ever-evolving threat landscape. Hackathons have been previously used as an approach to tackle these challenges. Hackathons are time-bounded events where participants with diverse backgrounds form teams and work on projects of interest to them (Pe-Than *et al.*, 2019). Hackathons in educational settings have been found to encourage students to practice the concepts learned in the classroom (Gama *et al.*, 2018; Byrne *et al.*, 2016; Oyetade *et al.*, 2022); thus, we perceive hackathons integrated into an educational setting can add practicability. In this regard, we explore the question:

RQ2. *How can hackathons be used for learning about IoT security risk management?*

To answer **RQ2**, we propose a hackathon approach to teach about IoT security risk management using the proposed IoTA-SRM framework. A hackathon learning model can help bridge the gap and increase the possibility of successfully implementing the framework in a real-world setting. We apply our approach in a cybersecurity course and analyze its outcomes, showing the usefulness of hackathons and their interventions in supporting learning about IoT security risk management (**RQ1**, **RQ2**). The remainder of our paper is organised as follows: First, in Section 2, we provide the background of our work and describe our research method in Section 3. We present the IoTA-SRM framework in Section 4, to answer **RQ1** and the hackathon learning model in Section 5, to answer **RQ2**. In Section 6, we evaluate the benefits of these artifacts (**RQ1**, **RQ2**) discussing the research implications and the limitations of our work in Section 7. Finally, in Section 8, we provide conclusions and future work. Our results indicate that our IoTA-SRM framework can guide multi-layer security risk management in IoT systems

in real-world scenarios and provide consistent security analysis outcomes. Additionally, we saw benefits in our hackathon approach to teach participants how to apply the proposed framework, thus supporting learning about IoT security risk management.

2. Background

In this section, we discuss the IoT system architecture as the basis for our IoTA-SRM framework and explore security risk management approaches that guide the framework. We also explore hackathon approaches that can be applied to facilitate learning how to apply our proposed framework.

2.1. *IoT System Architecture Perspective to Security Risk Management*

The IoT system architecture covers how software and hardware components act and work mutually in gathering, processing, storing, distributing, and using information from distributed sources to perform specific tasks and make decisions that meet their design objectives (Affia *et al.*, 2021; Lombardi *et al.*, 2021). Due to the heterogeneous nature of IoT components, each of which depends on different design specifications and system requirements, no standard approach for IoT deployments fits all use-cases (Kumar and Mallick, 2018). Thus, many well-known international organizations and working groups have presented IoT architecture frameworks based on differing application requirements, network topology, protocols, and business and service models (Lombardi *et al.*, 2021). The most commonly used architectures include the three-layer, four-layer service-oriented architecture (SOA), the middleware-based IoT or five-layer architecture and Cisco's seven-layer IoT architecture (illustrated in Fig. 1) (Swamy and Kota, 2020; Lombardi *et al.*, 2021; Kumar and Mallick, 2018).

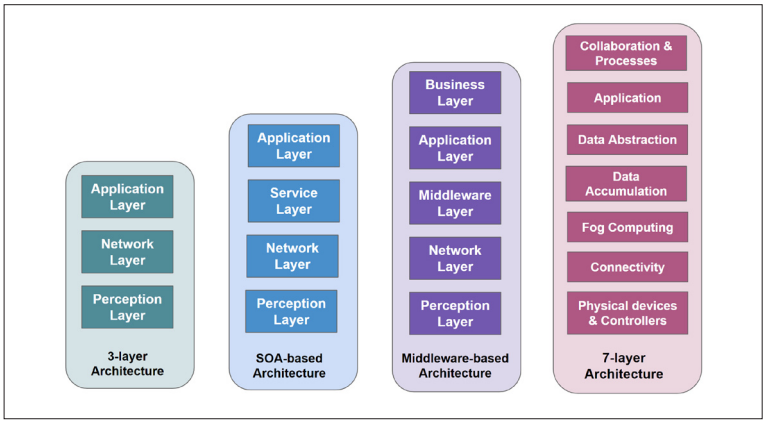

Fig. 1. Common IoT architectures (Swamy and Kota, 2020; Lombardi *et al.*, 2021; Kumar and Mallick, 2018).

Although architectures beyond the basic three-layered architecture seek to cover, in more detail, aspects of integrating wider technology and application areas and their implications on the business value in a service-oriented world (Kumar and Mallick, 2018), these architectures are built upon the three-layer model. We discuss the layers below:

- **Perception layer:** The perception layer of an IoT system provides capabilities for detecting, communicating, and collecting information about the environment without human interaction. These objects are internet-connected, uniquely identifiable, and can initiate communication autonomously (Wu *et al.*, 2010).
- **Network layer:** The network layer in an IoT system facilitates the transmission and processing of information between networked IoT perception objects, other devices, infrastructure, or application layer objects and services. Depending on the use case, various network protocols such as CoAP, Zigbee, 3G, LAN, Bluetooth, RFID, or NFC (Kumar and Mallick, 2018) can be used. Additionally, the network layer comprises the communication infrastructure and supporting protocols allowing end-users and objects to interact (Affia *et al.*, 2021).
- **Application layer:** The main feature of this layer is to deliver application-specific services to the end-user based on the application type, set business and profit models, and information provided from perception objects. Depending on the use case, this layer can include service-oriented technologies like cloud computing, storage, integrations to other applications, etc., to perform activities required by the end-user (Schiller *et al.*, 2022; Lombardi *et al.*, 2021).

2.2. *IoT Security Risk Management*

Security risk management in IoT systems requires a comprehensive understanding of the system's assets, their relationships with each other, and their vulnerabilities and potential risks. A model-based approach to security risk management can provide a systematic and repeatable method for identifying, evaluating, and mitigating security risks, ensuring that allrelevant aspects of thesystem,including technical and non-technical factors, are considered. Asset identification and functional decomposition are also significant processes that help break down the system into smaller, more manageable components and identify the assets that require protection. In Table 1, we explore various security risk management methods that can be applied in IoT systems,

Table 1

Criteria for comparing different security risk management methods

Criteria	ISSRM	OCTAVE	NIST	TARA
Support for Asset Identification	++	+–	+–	––
Support for Functional Decomposition	++	+–	+–	++
Model-Based Security Risk Management	++	+–	––	––

[++] Full fulfillment, [+–] Partial fulfillment, and [––] No fulfillment

highlighting their strengths and limitations for IoT security risk management following the asset identification, functional decomposition, and model-based security risk management criteria.

- The National Institute of Standards and Technology (NIST, 2002) approach supports information security risk management by identifying threat sources and events, identifying the vulnerabilities that might be exploited and the respective likelihood and impact of threat events, and then determining risks posed to the system. In its special publication 800-213A, NIST proposes cybersecurity requirements for devices and provides different assessments based on device type and capabilities (Fagan *et al.*, 2021). While the NIST approach provides normative guidelines for security risk management, but it does not have a specific focus on asset identification. It identifies threat sources and events, vulnerabilities, likelihood, and impact of threat events but does not systematically identify system assets.
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation Method) risk management approach (Caralli *et al.*, 2007) follows: (1) establishing criteria for risk assessment and measurement, (2) identification and profiling of assets, (3) identification of vulnerabilities and threats of primary assets, and (4) risk assessment and development of mitigation strategies. OCTAVE emphasizes identifying critical assets first (Ali and Awad, 2018) and then expanding based on how those assets can be threatened and the risk that develops. OCTAVE recognizes the need for asset identification but does not provide clear guidance on this process. It emphasizes identifying critical assets first and then expanding based on how they can be threatened and the risk that develops.
- MITRE's "Threat Assessment & Remediation Analysis" (TARA) approach (Wynn *et al.*, 2011) focuses on (1) breaking down prospective attacks into a manageable list of probable attacks and (2) communicating risks and recommendations to the organization. TARA was developed in response to a need to assess the security risks in the complex, quickly evolving threat landscape (Kandasamy *et al.*, 2020). The TARA approach focuses on breaking prospective attacks into a manageable list of probable attacks and communicating risks and recommendations to the organization. However, it does not systematically identify system assets.
- ISSRM is a model-based Information System Security Risk Management (ISSRM) approach (Mayer, 2009) proposed a conceptual reference model for security risk management called the domain model, defining asset, risk and risk treatment-related concepts for security risk management. management (Affia *et al.*, 2021). The ISSRM method acknowledges the importance of asset identification and provides concrete concepts, defines relationships between asset-related concepts, and presents a model-based process for security risk management. This makes it particularly promising for systematic asset identification and functional decomposition of the system as an input to security risk analysis and treatment. However, it may require more effort to implement the ISSRM method due to its model-based approach.

Based on our analysis, we explore the ISSRM method for further consideration in supporting IoT security risk management. The ISSRM method covers three major security risk management concept groups: asset-related, risk-related, and risk treatment-related concepts (Dubois *et al.*, 2010).

Asset-related concepts describe constructs for critical business and information system (IS) assets to protect, and the security criteria guarantee a certain level of asset security (in terms of confidentiality, integrity, and availability). *IS assets* are components of the system (e.g., hardware, software, or network) that support *business assets* (i.e., information, data, and processes) that bring business value. *Security criteria* determines the level of asset security (confidentiality, integrity, and availability) defined for each identified *business asset*. Activities *(a), (b)* in Fig. 2 cover asset-related concepts.

Risk-related concepts introduce constructs for security risk itself and its components (threat, vulnerability, risk impact, etc.). A *vulnerability* constitutes the weakness of the *IS assets*. A *threat* thus exists when an entity with interests can exploit a vulnerability to harm the *IS assets* and negate the *security criteria* of the *business assets*. The security *risk impact* are the negative consequences of the event where a *threat* exploits one or more *vulnerabilities*. Activity *(c)* in Fig. 2 cover risk-related concepts.

Lastly, *risk treatment-related* concepts describe constructs to treat risk, including the risk treatment decision, security requirements, and the controls that implement the defined security requirements. *Security requirements* are the conditions to be reached by mitigating the security risks. Following these requirements, we can implement security *controls* to treat the identified security risks. Activities *(d), (e), (f)* in Fig. 2 cover risk treatment-related concepts.

We consider using the ISSRM method as the theoretical foundation of our framework (see Section 4). Our proposed framework can leverage the key elements of ISSRM to provide a structured and effective approach to IoT security risk management based on the system's underlying architecture. However, while ISSRM is preferred for analysing IoT systems from an architectural perspective, OCTAVE and TARA can also be useful in specific contexts.

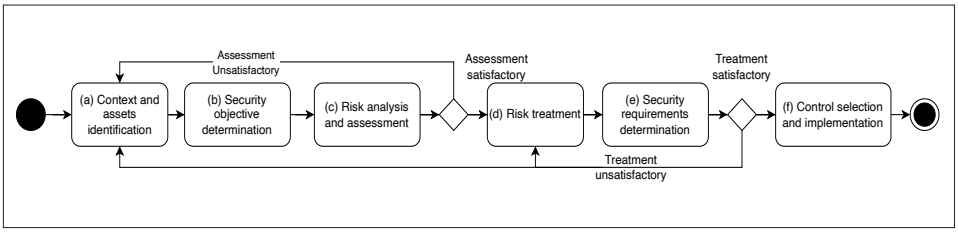

Fig. 2. ISSRM process adapted from Matulevičius (2017); Dubois *et al.* (2010).

2.3. *Hackathon Model for Security Learning*

Studies suggest that practical-oriented education strategies can improve learning outcomes in cybersecurity by mastering cybersecurity fundamentals (Crumpler and Lewis, 2019), building hands-on skills and experience (Crumpler and Lewis, 2019; Kam and Katerattanakul, 2019), employing adversarial and system thinking (Hamman and Hopkinson, 2016), and building soft skills (i.e., communication, problem-solving, collaboration, and team working) (Crumpler and Lewis, 2019; Hamman and Hopkinson, 2016). Hackathons have been proposed as suitable for implementing these strategies, particularly in providing targeted learning content, introducing real-world scenarios and gamification, and encouraging an adversarial thinking approach (Affia *et al.*, 2022; Karagiannis and Magkos, 2020; OConnor and Stricklan, 2021; Cheung *et al.*, 2011). Additionally, hackathons provide flexible arrangements and mentoring opportunities (Wang and Sbeit, 2020; Affia *et al.*, 2022).

However, hackathon approaches that support learning about applying security risk management are limited compared to capture-the-flag or competition-based hackathons (Li and Kulkarni, 2016), which are insufficient to support security risk management learning. CTF or competition-based hackathons target direct system vulnerability identification and exploitation but fail to achieve the granularity needed for a more thorough asset-oriented system analysis as an input to risk analysis and then providing constructive recommendations for security risk management. Additionally, while hackathons are a good approach to encourage learning-by-doing, such benefits cannot materialize without careful planning to create a suitable learning environment within the hackathon context (Affia *et al.*, 2020). To support security analysis using our proposed IoT security risk management framework, we have examined existing research on hackathon designs for learning, as detailed in Section 5.

Nolte *et al.* (2020b) proposed a hackathon planning kit[1] that outlines 12 major decision points to consider when organizing hackathons for specific outcomes. Careful planning of the hackathon goals, theme, competition/cooperation style, duration, agenda, and other specialized preparations (Nolte *et al.*, 2020b) contribute to a successful hackathon event for participants, allowing them to develop practical skills in security and apply gained knowledge in the real world (Cheung *et al.*, 2011; OConnor and Stricklan, 2021). Affia *et al.* (2020, 2022) have proposed hackathon interventions to drive learning-oriented benefits within the hackathon events. Hackathon interventions focus on design actions that pair the existing difficulties in security learning to suitable hackathon design aspects to achieve learning outcomes (Kollwitz and Dinter, 2019).

Finally, it's important to note that hackathon participants must become proficient in the basics of security risk management, which can be complex and require breaking down into smaller components to facilitate learning and practice (Crumpler and Lewis, 2019; Affia *et al.*, 2022). Therefore, a hackathon design that enables organizers to iteratively execute their model around the connected parts of a split topic is also crucial.

[1] `https://hackathon-planning-kit.org/`

3. Research Method

Our research method is two-fold to answer our research questions (**RQ1** and **RQ2**). We first identified the limitations of existing security risk management approaches in addressing the unique characteristics of IoT systems, such as the architecture perspective (see Section 2). To address this problem, we learn from existing IoT and security domain analysis to develop the IoT architecture-based Security Risk Management (IoTA-SRM) framework taking a comprehensive approach to managing risks in IoT systems (**RQ1**). Additionally, we recognize the need for practical learning models for cybersecurity professionals to apply the framework effectively. This led us to develop a hackathon learning model to teach professionals how to use the IoTA-SRM framework to build secure IoT systems (**RQ1**, **RQ2**). We then evaluate the benefits of these artifacts in real-world settings using action research. Integrating the hackathon learning model into a cybersecurity course provides an opportunity to apply the IoTA-SRM framework in a practical setting and assess the learning outcomes for the students. Through our action research study, we design hackathon interventions suitable for our setting as a mode of delivery of our framework and provide support to hackathon participants at each hackathon event.

3.1. *Framework Creation*

In Section 2, we conducted a background analysis by reviewing existing literature on IoT architecture. We selected the three-layer architecture providing a theoretical foundation for our framework. Its simplicity renders it easy to comprehend and execute, making it advantageous for organizations lacking technical expertise or resources to

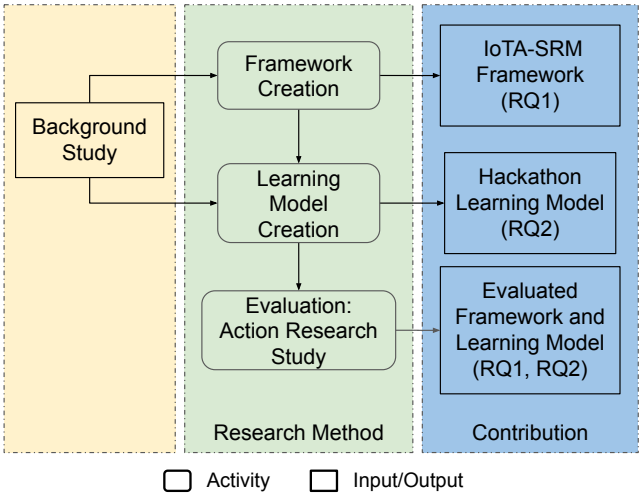

Fig. 3. Study Design.

adopt and use in security risk management activities. Using relevant system modelling concepts from Angermeier *et al.* (2016), we can iteratively define components and other conceptual abstractions to develop a comprehensive view of the system's layers that existing security risk management approaches do not fully consider. After analyzing several security risk management methods for IoT systems in Section 2.2, we selected the ISSRM method and its process (see Fig. 2) to guide our framework's security risk management concepts and the threat-driven approach (Affia *et al.*, 2019) to guide systematic threat analysis.

This process derives four core activities supported by domain-specific outputs and guidelines. The first step is to model the system, which involves breaking it down into logical layers, analyzing it by components, and defining asset-related security concepts.

The second step is to discover risks by identifying and evaluating potential security threats using a threat-driven approach. The third step is to handle risks by making decisions to treat security risks based on security requirements, typically expressed in decision terms. Finally, the fourth step is to analyze tradeoffs, which involves evaluating the trade-offs between available resources and the effort required to respond to identified risks and implement risk controls. It is important to note that these activities are iterative and may be revisited as needed, as the process is guided by an ongoing risk management cycle. We discuss the results of our framework creation in Section 4.

3.2. *Hackathon Learning Model Creation*

We identified the need for practical learning models to teach cybersecurity professionals how to apply the IoTA-SRM framework effectively. We learned from existing work by Affia *et al.* (2020, 2022) that proposed hackathon interventions to drive learning-oriented benefits and Nolte *et al.* (2020b) who provided guidelines for organizing hackathons, to inform the design of our model. Based on this review, we designed hackathon interventions for each event to facilitate the use and delivery of learning content and support other aspects of learning during the hackathon (**RQ2**). We designed the learning model to use multiple hackathon iterations to address the complexity of learning security risk management concepts. The iterations were focused on teaching the core activities of the IoTA-SRM framework, which were split into standalone yet connected components. At the end of each hackathon activity, participants produced hackathon artifacts following each IoTA-SRM activity. These artifacts were then used as a means of assessing the learning progress of participants.

3.3. *Evaluation: Action Research*

In our study, we adopted the action research method (Lewin, 1946) to assess the effectiveness of the hackathon learning model in teaching the IoTA-SRM framework. To do

so, we integrated the hackathon learning model (described in Section 5) into a cybersecurity course covering secure software development from a security risk-aware perspective and introduced the IoTA-SRM framework. The participants in our study were cybersecurity students with varying levels of prior knowledge in cybersecurity and from diverse backgrounds. Within the course setting, we presented an IoT use-case, which is described in Appendix A, that allowed the students to apply the IoTA-SRM framework activities.

After each hackathon event, we developed survey instruments that included pre-existing Likert scales and open-ended questions, as detailed in Appendix B. The Likert scales were used to measure the perceived usefulness of each hackathon intervention (Sauro, 2011), the ability of the hackathon interventions to contribute to learning (García-Hernández and González-Ramírez, 2018), and the satisfaction of the students regarding the interventions, all of which contributed to answering **RQ2**.

Finally, we analyzed the data collected after each hackathon event, including the responses to the open-ended questions, to complement the Likert scales and support our arguments in answering **RQ2**. We selected responses from seven (7) teams based on their size (with at least two (2) members who provided more complete responses to the questionnaires). To ensure the reliability and consistency of our data, we transformed the data collected from the Likert scale into a numerical format ranging from 1–5. We assigned unique codes to each question scale to facilitate further data preparation and analysis. To examine the internal consistency of the coded questions, we applied Cronbach's Alpha to calculate the alpha coefficients for scales measuring the interventions and learning-related concepts at each hackathon and the entire questionnaire. We only selected scales where Cronbach's Alphas were higher than the acceptable value of 0.70 (Gliem and Gliem, 2003), thus supporting internal consistency and reliability.

Our findings, presented in Section 6, show the impact of hackathon interventions in encouraging hands-on learning and achieving learning outcomes related to IoT security risk management. Moreover, we demonstrate the application of the IoTA-SRM framework in a real-world context when integrated into the hackathon learning model.

4. IoT Architecture-Based Security Risk Management (IoTA-SRM) Framework

This section discusses our findings from implementing our research method to create the IoTA-SRM framework.

4.1. *Conceptual Model*

The IoT architecture can be broken down into $component$ elements with sub-element relationships, $functions$, $dataElements$, and $dataFlows$. This allows for the establishment of hierarchies and the illustration of risk-related and risk-treatment-related con-

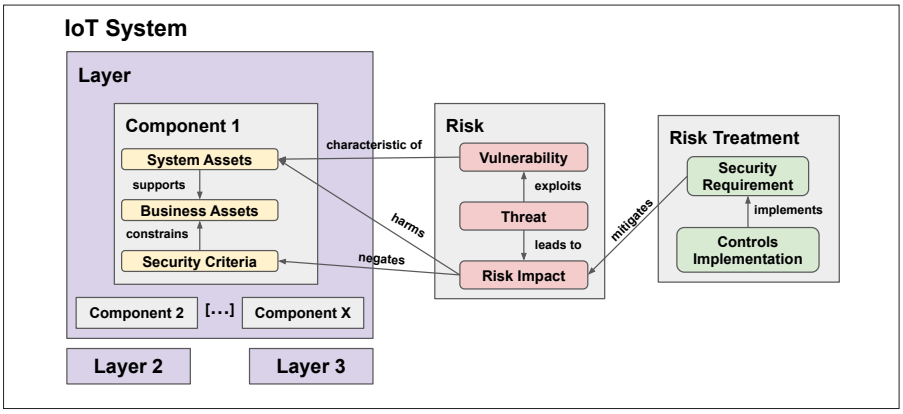

Fig. 4. IoTA-SRM Conceptual model.

cepts and interactions. Each component and sub-element can have a vulnerability and a threat, which can help determine the risk impact at each layer. Security requirements are defined for each layer, and security controls are implemented to address the identified security risks. We illustrate the conceptual model in Fig. 4.

4.2. *IoTA-SRM Framework Process*

Our IoTA-SRM framework features four core activities (see Fig. 5) to guide IoT security risk management, each supported by guidelines and domain-specific outputs.

4.2.1. *Model System*

This activity involves describing the IoT system's comprehensive abstraction and interactions within the system, breaking it down into logical layers, analyzing it by components, and defining asset-related security concepts. The asset-related concepts of the IoT system are the *component* elements and their sub-elements, considered as *IS assets* at each IoT layer. A *component* can be any physical or virtual object that supports the necessary functions of the IoT system in data handling, data flow through the system, and data life cycle in the system. For example, we can decompose the perception layer

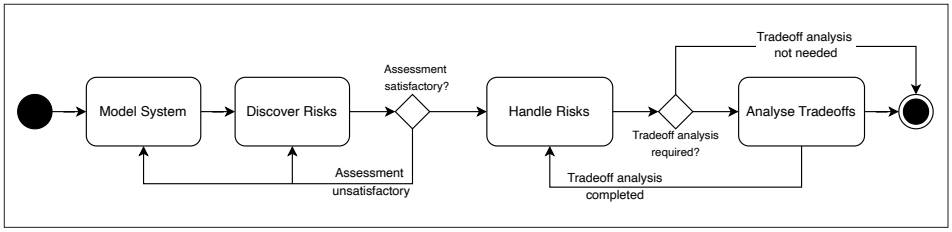

Fig. 5. IoTA-SRM Framework Procedure.

into sensing, visioning, positioning, and actuating components where we identify the GPS $component$ (system asset) within the positioning component.

Business assets are the $functions$, $dataElements$, and $dataFlows$ that provide business value and are supported by the *IS assets*. Data elements represent important business data supported by IoT components to deliver the intended IoT business service. Functions refer to the various data processing and transmission tasks required by the system, which are executed by components and dependent on them. Each data flow has a corresponding sender and receiver component, representing data flow between system components. For example, in an autonomous car, the GPS component can transmit the collected telemetry data element through the network layer components to the navigation component in the application layer. Once the assets are derived, we can determine the level of protection required for the business assets based on their *security criteria*, defined in terms of confidentiality, integrity, and availability (CIA) of the business assets. For instance, in autonomous vehicle systems, all telemetry data collected by the GPS component must be transmitted without being corrupted to an application layer component to ensure safe driving and navigation of the autonomous car.

The results of this activity are a complete asset list, a system model illustrating the interaction between the assets involved in the IoT use case, and security objectives denoting the importance of the business assets. It is important to document the outcomes of this activity properly.

4.2.2. *Discover Risks*

In this activity, we identify and evaluate potential security threats that may exploit vulnerabilities in the IoT system's components and cause harm to the system's IS assets (denoted as $components$) and its business assets (denoted as $functions$, $dataElements$, and $dataFlows$). This activity involves using adversarial thinking and creativity to conduct multi-layer vulnerability analysis and threat modelling from the perspective of a malicious actor or user. Vulnerability analysis can be done using vulnerability resources (NVD, a; CWE, a; OWASP, 2021). Thus at each IoT layer and for each component, we can identify vulnerabilities for further security analysis depending on the level of abstraction in the analysis. For example, a GPS tracker *system asset* can have a broken authentication vulnerability causing it to execute SMS-based GPS commands without authentication (CVE-2022-2141)[2]. Once we have identified the vulnerable system assets, we can discover security threats using the STRIDE method[3] for security risk management (Affia *et al.*, 2019).

The impact of security risks in each IoT layer can result from attacks within that layer or in other layers, creating a ripple effect of risk impacts across multiple layers. Therefore, it is crucial to consider the potential risk impacts across various IoT layers. For instance, if an unauthorized GPS command action occurs at the perception layer, it can tamper with the analysis of legitimate tracking data sent to the computing system asset at

[2] `https://nvd.nist.gov/vuln/detail/CVE-2022-2141`

[3] STRIDE stands for *Spoofing (S)*, *Tampering (T)*, *Repudiation (R)*, *Information Disclosure (I)*, *Denial of Service (D)*, and *Elevation of Privilege (E)* (Shostack, 2014).

the application layer of the IoT system. This type of security risk can pose a significant impact on critical applications.

The outcomes of this activity include vulnerability and threat lists, as well as information on the impact of risks (see Table 2). It is essential to document the results of this activity appropriately.

4.2.3. *Handle Risks*

This activity involves making decisions to treat security risks based on the risks identified in the *Discover Risks* activity, typically expressed in decision terms (avoidance, reduction, transfer, retention) made by IoT system stakeholders. If the decision is to reduce the risk, security requirements must be defined to guide the implementation of security controls to mitigate risks. Here we propose incorporating the STRIDE security requirements (confidentiality, integrity, availability, authentication, authorization, and non-repudiation/auditability) to guide the security requirements definition for the system (Affia *et al.*, 2019). For example, an authentication security requirement can prevent attackers from accessing the GPS asset to falsify tracking data. The security controls implement the defined security requirements to treat the identified security risks and create a more secure system state. For example, a strong password-based authentication security control can be implemented for the GPS device system asset before allowing access to its functions. However, the decision on implementation requires analytical reflection on the discovered risks to produce effective remediation plans guided by a tradeoff analysis (see Section 4.2.4). The main outcomes of this activity are the defined security requirements and suggested controls to treat the identified risks. It is important to document the outcome of this activity appropriately.

Table 2
IoTA-SRM activity tasks and outcomes

Activity	Activity Tasks	Outcome Artifacts
Model System	Decompose IoT system into IoT layers	
	Identify system and business assets for each IoT layer	Asset list
	Define security objectives for business assets per IoT layer	Security objectives
	Model decomposed system	Asset model
Discover Risks	Multi-layer vulnerability assessment	Vulnerability list
	Multi-layer threat elicitation	Threat list
	Multi-layer risk impact estimation	Risk impact information
Handle Risks	Multi-layer risk treatment decision	Risk decision
	Security requirements elicitation	Security requirements
	Control selection	Selected controls list
	Control implementation (can follow *Analyse Tradeoffs* outcome)	
Analyse Tradeoffs	Determine asset values from *Model Risk* activity	Asset metric values
	Estimate risk impact values from *Discover Risks* activity	Risk impact metric values
	Estimate selected controls costs from *Handle Risks* activity	Control cost metric value
	Run cost vs benefit analysis for risk reduction	Prioritized risk list

4.2.4. *Analyse Trade-offs*

Mitigating risks in IoT systems through implementing security controls can be resource-intensive, requiring considerable time, money, and technical expertise. As organizations may not have sufficient resources allocated for IoT security risk management, evaluating the trade-offs between the available resources and the effort required to respond to identified risks and implement risk controls becomes crucial. To prioritize risks based on their potential impact and available resources, we propose a security metric and trade-off analysis procedure to assist in managing resources for security risk treatment. This compiles metric values of assets from the *Model System* activity, risk impact estimation from the *Discover Risks* activity, cost of implementing controls as well as risk reduction levels as a result of the suggested controls in the *Handle Risks* activity are collected to analyze the trade-offs. The main outcome of this activity is the prioritized risks whose selected controls will be implemented to secure the system (see Table 2). Additionally, we encourage appropriate documentation of the outcome of this activity.

5. Hackathon Learning Model to Support IoT Security Risk Management Learning

Our hackathon learning model consists of multiple hackathon iterations where we teach how to apply each activity of the IoTA-SRM framework (Fig. 6). Each hackathon includes interventions as a mode of delivery for provided *learning content* supported by corresponding hackathon *tasks*. The outcome of each hackathon event is an *artifact* that learners iteratively improve over time.

5.1. *Iterative Format (Hackathon)*

The IoT security risk management framework in Section 4 covered four major activities: *Model System*, *Discover Risks*, *Handle Risks*, and *Analyse Tradeoffs*. These activities provided a basis to split learning about security risk management into standalone yet connected components, forming the iterative container of our learning process (i.e., an in-

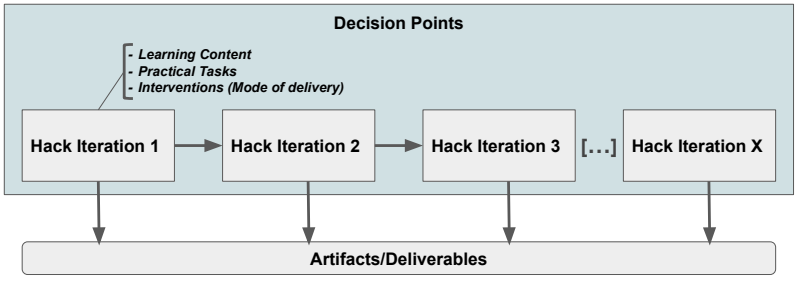

Fig. 6. Hackathon Learning Model.

stance of a hackathon). Within each iteration, we learn from the IoT security risk management framework and knowledge of the system context to refine the course lecture content and practical tasks introduced through interventions. Each iteration leads to the creation of artifacts and contributes to building secure IoT systems (as a learning outcome).

5.2. *Learning Content*

The learning content covers the IoT domain context, theoretical concepts related to each activity in our IoTA-SRM framework in Section 4 split between each hackathon event, and corresponding tasks that can be used to practice the concepts taught and produce hackathon *artifacts* (see Table 2). The IoT domain context is a real-world input for analysis that provides information on IoT system assets, their supported business assets of value, and the multi-layer interactions between assets to achieve the IoT service/application business goals. The IoTA-SRM framework then provides a structure by which we can conduct security risk management in the IoT system context. Based on the IoTA-SRM framework activities, we can introduce tasks to help students practice what they have learned. Table 2 illustrates major tasks that can be adapted to the selected IoT use case to perform each risk management activity and produce its outcome artifacts.

5.3. *Interventions (Mode of Delivery)*

Hackathon Interventions can be introduced as a mode of delivery for the *learning content* and to encourage the use of the *learning content*, provide expert support during the hackathon process, and support learning-by-doing at the hackathon events. Learning from Affia *et al.* (2022) and Nolte *et al.* (2020a), we propose the *thematic input* and *targeted feedback* interventions.

1. **Thematic Input:** Thematic input comprises all resources providedto inspire participants to reflect on the context under study and apply theme-specific knowledge (content) to achieve the outcome of the practical tasks. Carefully introduced thematic input builds hands-on skills/experience and encourages adversarial and system thinking (Crumpler and Lewis, 2019; Hamman and Hopkinson, 2016) in hackathon participants.
2. **Targeted Feedback:** One of the most prevalent forms of learning-oriented support during a hackathon is the inclusion of mentor or peer feedback opportunities, especially when the mentors perceive their role as that of a traditional (workplace or educational) mentor (Nolte *et al.*, 2020a; Rukmono and Chaudron, 2022). The organization of feedback should encourage ample mentor-team interactions. In Affia *et al.* (2022), mentor feedback helped to clear up misunderstandings and errors in hackathon tasks, improve teamwork and encourage rapid learning by helping teams work together to complete tasks correctly. Feedback is also crucial to ensure students do not continue with a wrong understanding of the introduced concepts at future hackathons (Affia *et al.*, 2022).

5.4. *Hackathon Artifacts*

During each hackathon, participants will develop artifacts (highlighted in Table 2) as outcomes of each activity in the developed framework. *Model system* outcomes include (system and business) asset list, an asset model illustrated using an appropriate modelling language, and security objectives understanding the importance of the business assets. *Discover risks* activity outcomes include multi-layer vulnerability, threat and risk impact analysis. *Handle risks* activity outcome covers the prioritized risks whose selected controls will be implemented to secure the system and appropriate documentation of the activity. Lastly, the *Tradeoff analysis* activity outcome is the prioritized risks whose selected controls will be implemented to secure the system and appropriate documentation of the activity.

5.5. *Hackathon Learning Model Application*

We apply the hackathon learning model in a cybersecurity course focused on a security risk-aware perspective to secure software design covering security of software system assets, security requirements engineering and modelling, and understanding major security controls, consistent with the IoTA-SRM framework in Section 4. The hackathons were facilitated by the course instructors and designed based on the activities outlined in the IoTA-SRM framework, with specific goals, agendas, and durations as highlighted in Table 3. These hackathons focused on three of the IoTA-SRM framework activities

Table 3

Method Setting for each Hackathon Iteration

Decision Points	
Goal	Learn how to apply IoT security risk management. Build secure IoT systems by applying IoT security risk management. Produce security assessment artifacts and secure system models
Duration Agenda	*Approx* 48 hours split over 14 days See Fig. 7
Specialized preparation	IoT system context provided as a micro-mobility use-case Cybersecurity course design
Learning Content	
Learning content	Course lecture materials Framework proposed in Section 4 IoT system context use-case document
Tasks	See Table 2
Interventions	**(mode of delivery)**
Thematic input Targeted	Lectures
Feedback	Mentor feedback (with course instructors as mentors)
Artifacts	
	Practical task outcomes at the end of the hackathon iteration
	Hackathon (risk management) report

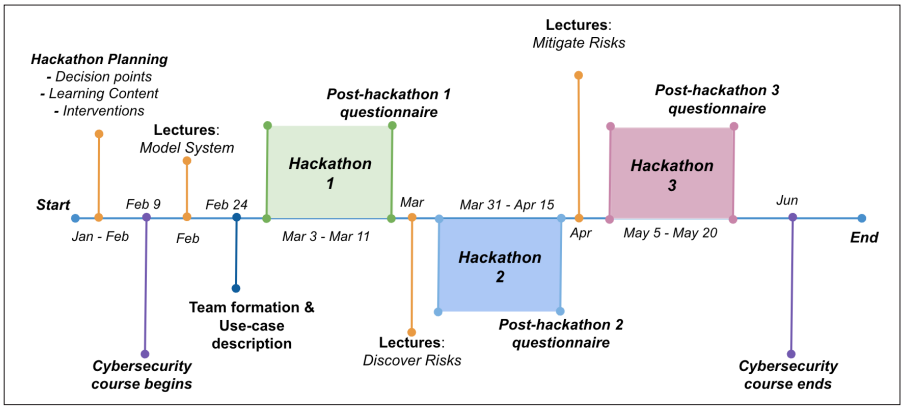

Fig. 7. Timeline of activities.

and were conducted within the duration of the cybersecurity course. To provide a practical scenario for analysis, the course instructors provided a micro-mobility software-intensive IoT system use-case (see Appendix A) along with UML diagrams and textual descriptions. At the beginning of the course (see Fig. 7), the hackathon format was introduced, requesting students to form teams of three (3) or four (4) members.

To facilitate learning during the hackathon events, we developed two hackathon interventions. The first intervention – the *lecture* intervention – offers thematic input support through specially designed lecture sessions. The second intervention – the *feedback* intervention – provides targeted feedback through mentoring and multiple mentor feedback interactions. We discuss how these interventions apply within the IoTA-SRM framework activities used in this setting.

5.5.1. *Model System Hackathon (Hackathon 1)*

We organized the first iteration of the hackathon learning model (see Section 2.3) about two (2) weeks after the start of the course. This initial hackathon event (*Hackathon 1* in Fig. 7) was based on the *Model System* IoTA-SRM activity. The hackathon tasks involved having the students define the system context and scope of the scooter use case, perform system architecture and asset analysis and analyze the security objectives of the assets in scope. At the end of the hackathon, we requested the students to submit a security asset analysis report of the IoT use case as the hackathon artifact.

- **Lecture Intervention:** We provided base knowledge through lectures and lecture resources to the student teams to inspire participant reflection on their IoT system case and apply the introduced concepts in completing the hackathon tasks. The lectures were crucial, especially at the start of the course, to provide the foundational knowledge needed by the students to derive the business assets, system assets, and security objectives of the IoT system case.
- **Feedback Intervention:** Participants submitted a hackathon report as the outcome artifact at the end of the hackathon. The course instructors provided written

feedback on the submitted report, correcting mistakes and offering suggestions for improvement. The feedback was detailed to enhance understanding of the introduced concepts and support better performance in future hackathon iterations.

5.5.2. *Discover Risks Hackathon (Hackathon 2)*

About a month after Hackathon 1, we conducted the second hackathon event (*Hackathon 2* in Fig. 7). We assigned hackathon tasks to the students to perform security threat elicitation, vulnerability assessment, and risk impact estimation on the analysis outcomes of the Model System activity (from *Hackathon 1*). We also guided comprehensive risk documentation by offering risk templates to follow. At the end of the hackathon, we requested the students to submit a security risk analysis report of the IoT use case as the hackathon artifact.

- **Lecture Intervention:** Before the second hackathon, we provided the second round of lectures which covered *risk-related concepts* of software systems before the event. We provided base knowledge through the lectures and lecture resources to the student teams to help complete the hackathon tasks. We guided practical vulnerability assessment and threat elicitation through additional lecture resources showing examples that can apply to the scooter (IoT) use case domain.
- **Feedback Intervention:** For the second hackathon, we introduced online consultation feedback to reinforce correct understanding of the concepts introduced in the lectures and lecture resources. These online sessions allowed for ad-hoc feedback based on student or team requests, fostering a more interactive engagement between mentors and student teams. At the end of the hackathon, the teams participated in presentation sessions to discuss the outcomes of their tasks and receive feedback from mentors and other teams. Mentors provided additional written feedback on the submitted hackathon artifacts.

5.5.3. *Handle Risks Hackathon (Hackathon 3)*

We organized the third and final hackathon event (*Hackathon 3* in Fig. 7) about a month after *Hackathon 2*. We provided hackathon tasks to practice handling and treating the risks discovered during the *Discover Risks* activity. The hackathon tasks include security requirements elicitation and modelling role-based access control. We asked the students to submit an overall security risk management report of the IoT use case accumulating all analyses conducted at all three hackathon iterations.

- **Lecture Intervention:** Before this event, we provided the third round of lectures, emphasizing the practice of security requirements elicitation and modelling role-based access control.
- **Feedback Intervention:** We continued with the online consultation session format to discuss task progress or challenges with the final hackathon tasks. The teams participated in presentation sessions at the end of the hackathon event, where mentors provided feedback on the work done and recommendations for completing their cumulative hackathon report. As this was the final hackathon, we did not provide further written feedback to the students.

6. Evaluation Results

In our action research study, our interest is in the perceived impact of the developed hackathon learning model introduced into a cybersecurity course to teach professionals how to apply the framework to build secure IoT systems.

During data pre-processing, we found that the calculated Cronbach's Alphas for summated scales of Likert-scale items measuring the interventions and learning-related concepts were above the acceptable value of 0.70 (Gliem and Gliem, 2003), indicating internal consistency and reliability of our survey instruments. Table 4 details the Cronbach's Alphas for the summated scales of each Likert-scale item at each hackathon event, using human-readable names, such as the *Lecture* intervention scale. We used the summated scales of each Likert-scale item for further data analysis, which included descriptive statistics of central tendency and dispersion using the median and interquartile range due to the ordinal level of measurement. The descriptive statistics of our data sample, which included cybersecurity students from different backgrounds, are presented in Table 5.

Our findings indicate that students perceived the hackathon format to contribute to learning ($M = 4.0$, $IQR = 0.38$). This is also evident by C01 remarking that they *"learnt a lot"* (C01) while C03 explained that it was *"a different approach using hackathons"* (C03). When analysed across all three hackathons, we saw that the perception of the lecture interventions' contribution to learning at the hackathons steadily but consistently rose through all three hackathons (Hackathon 1: $M = 3.58$, Hackathon 2: $M = 3.77$, Hackathon 3: $M = 4.03$).

Table 4
Internal Consistency of Collected Datapoints at the Hackathons

	Cronbach's α
Model System Hackathon (n=20)	
Lecture Intervention	0.90
Written Feedback Intervention	0.84
Discover Risks Hackathon (n=20)	
Lecture Intervention	0.83
Written Feedback Intervention	0.84
Presentation Feedback Intervention	0.86
Online Feedback Intervention	0.81
Handle Risks Hackathon (n=20)	
Lecture Intervention	0.81
Presentation Feedback Intervention	0.87
Online Feedback Intervention	0.93
Hackathon Approach to Learning	0.74
Overall Interventions Learning Contribution (n=60)	
Overall Lecture Intervention	0.86
Overall Feedback Intervention	0.92

Table 5

Descriptive statistics of data points from all three (3) hackathon events. Median (M) and interquartile range (IQR) values are from responses on a 5-point Likert scale

Teams	Participants		**Interventions**					*Hackathon Approach to Learning
			Lecture	Feedback	Online Feedback	Written Feedback	Presentation Feedback	
A	A01, A02	M	3.35	3.26	3.27	3.35	3.27	3.58
		IQR	0.37	0.14	0.13	0.15	0.09	0.12
B	B01, B02 B03	M	3.62	3.77	3.85	3.73	3.81	4.00
		IQR	0.38	0.21	0.17	0.27	0.22	0.25
C	C01, C02 C03, C04	M	3.96	3.79	4.04	3.96	3.46	4.00
		IQR	0.23	0.41	0.36	0.28	0.42	0.10
E	E01, E02	M	4.42	4.40	4.58	4.35	4.23	4.83
		IQR	0.44	0.46	0.47	0.46	0.35	0.00
F	F01, F02 F03, F04	M	3.46	3.40	3.04	3.73	3.54	3.50
		IQR	0.42	0.29	0.20	0.32	0.22	0.06
G	G01, G02	M	4.00	4.31	4.12	4.31	4.35	4.25
		IQR	0.29	0.09	0.31	0.09	0.14	0.12
H	H01, H02, H03	M	4.46	4.18	4.00	4.35	4.08	4.50
		IQR	0.42	0.13	0.13	0.31	0.23	0.12

*Data points were collected once at the final hackathon event

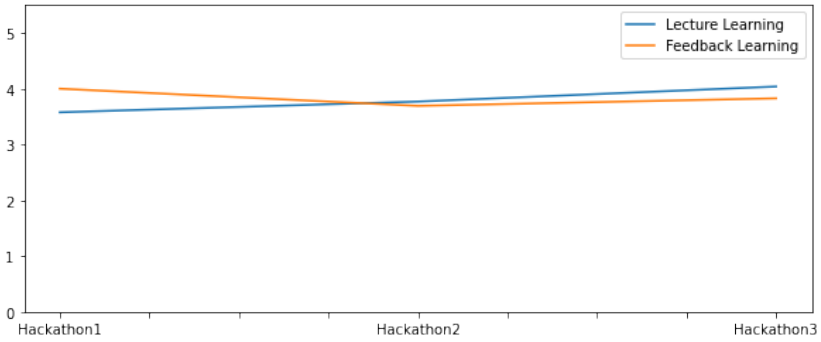

Fig. 8. Intervention contribution to learning the Hackathons.

The perception of the feedback interventions' contribution to learning at the hackathons slightly fell between Hackathon 1 ($M = 4.00$) and Hackathon 2 ($M = 3.69$) and narrowly rose at Hackathons 3 ($M = 3.83$). However, both interventions remained consistently positive across all three (3) hackathons. The positive and generally upward trend with both interventions thus indicates that our hackathon approach is beneficial for learning about IoT security risk management (**RQ2**).

In the following sub-sections, we analyze the student's perceptions in more detail and discuss how their perception evolved during the three hackathon iterations.

6.1. *Model System Hackathon*

According to our findings, students perceived both the lecture and feedback interventions as contributing to learning during the first hackathon. However, there was a higher perception of learning gains from the introduced written feedback intervention ($M = 4.00$, $IQR = 0.36$) compared to the lecture intervention ($M = 3.58$, $IQR = 0.55$). This could be because the detailed feedback helped correct misunderstandings of the introduced concepts.

Participant C03 highlighted the feedback as being *"very detailed.."* and *"very helpful"* (C03) for the team, while participant G04 was *"thankful for the detailed feedback"* (G04). Participants C01 and B04 also found the feedback valuable and helpful in improving their solutions. C01 added that *"in general feedback is highly valuable and gives a lot to understand what needs to be addressed in future"* (C01) and B04 added that the *"received feedback helped to improve my solution"* (B04). However, participant C01 suggested that *"maybe there would not be so much feedback if tasks were more detailed beforehand by setting precise goals and limits"* (C01). This can indicate the need for more detailed instructions for the hackathon tasks resulting in less need for feedback. Participant C03 also preferred consultation feedback, as many questions could not be addressed in one document. Participant C03 also highlighted that they *"would prefer consultation feedback more...* because *"there are a lot of questions..., and one document could not solve all of them"* (C03). This suggests that multiple forms of feedback could be beneficial for hackathon participants.

In terms of the lecture intervention, participants H04 found "*all lectures helpful"* (H04) while B04 expressed that the lectures "*helped to improve old knowledge in model constructing"* (B04). Participant C03 highlighted that the lectures helped them "*to understand the topic which was totally new"* (C03). Participant H03 preferred the practice lectures as they commented that they "*liked the practice lectures more, especially since we have to design something"* (H03). However, participant G04 felt that the lectures

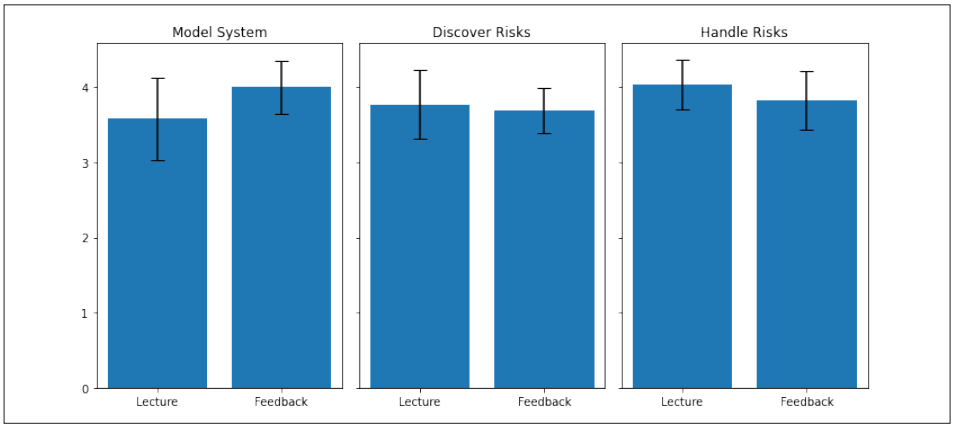

Fig. 9. Interventions contribution to learning at each hackathon.

sometimes caused an "*information overload"* (G04), making it "*extremely hard to follow and digest"* (G04), while Participant C04 found the delivery chaotic and note-taking difficult. This indicates that even with an attempt to split the content of the IoTA-SRM framework provided through the lectures into multiple parts, there is still a risk of information overload.

6.2. *Discover Risks Hackathon*

We found that the students perceived the lecture and feedback interventions contributed to learning during the hackathon. According to the data, the lecture intervention resulted in higher learning gains ($M = 3.77$, $IQR = 0.46$) compared to the feedback intervention ($M = 3.69$, $IQR = 0.30$), which was in contrast to the *Model System* hackathon. Fig. 10 shows the impact of feedback interventions on the hackathons. One possible reason for this difference is that the students realized the importance of having upfront information to perform better at the hackathon and tackle more complex tasks. C02 praised the lectures, stating that they are *"great"* and *"have very rich content"* (C02). Furthermore, as we provided offline versions of the lecture sessions, students could access them anytime for their convenience. C01 mentioned that they mostly relied on recorded lectures and that they give a *"better learning curve"* (C01). Thus, having prior knowledge of the learning content could be crucial for students to attempt the increasingly difficult tasks of the *Discover Risks* hackathon and enhance mentor-student discussions during feedback sessions. However, C02 also mentioned that they *"prefer if there was more time to consume the lecture contents at my own space and rhythm"* (C02).

Our study also showed that students had a positive perception of written feedback ($M = 3.92$, $IQR = 0.23$), online consultation feedback ($M = 3.62$, $IQR = 0.34$), and presentation feedback ($M = 3.54$, $IQR = 0.36$) contributing to their learning. Students

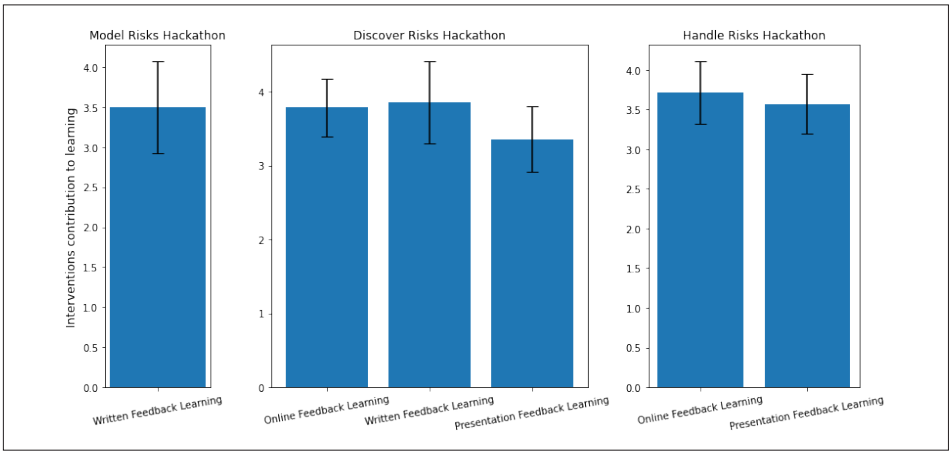

Fig. 10. Feedback Interventions at the Hackathons.

reported higher learning gains from the written feedback intervention than other feedback interventions, which could be attributed to the benefits of receiving detailed critiques of hackathon submissions. C02 emphasized that written feedback was especially helpful for their team as it was very detailed and helped them *"better understand shortcomings in our* [hackathon] *"report and easily fix the problems."* (C02). However, students also perceived online consultation and presentation feedback to positively impact their learning.

6.3. *Handle Risks Hackathon*

According to our findings, students perceived lecture and feedback interventions to contribute to learning during this hackathon. The students reported higher learning gains from the lecture intervention ($M = 4.04$, $IQR = 0.33$) compared to the feedback interventions ($M = 3.83$, $IQR = 0.39$), indicating an increasing perception of the lecture intervention's contribution to learning across all three hackathon events.

Although we did not conduct written feedback at this hackathon since it was the final submission, we introduced online consultation and presentation feedback interventions. Our findings revealed that students had a higher perception of the contribution to learning from the online consultation feedback ($M = 4.00$, $IQR = 0.41$) than the presentation feedback intervention ($M = 3.92$, $IQR = 0.35$). C03 remarked that after an online meeting, their confusion with the task was cleared, stating that the course instructors *"answered our questions"* (C03). On the other hand, C02 suggested that *"presentation feedback time could be a bit longer to make things easier to explain"* (C02), but C03 emphasized that they still *"personally prefer written form of the feedback"* (C03).

6.4. *Lessons Learned*

The study aimed to introduce the IoTA-SRM framework activities and tasks in Table 2 to students by breaking down the complex topic of security risk management and iteratively implementing framework activities in a hackathon model. The lecture and feedback interventions served as delivery modes for the IoTA-SRM framework. The hackathon tasks allowed students to independently construct knowledge and develop new insights into IoT security risk management.

Integrating the IoTA-SRM framework in the cybersecurity course yielded several valuable lessons. Firstly, the framework proved to be a useful tool for guiding students towards producing desired outcomes. With the aid of the IoTA-SRM framework, students developed a structured approach for identifying and analyzing security risks and vulnerabilities in IoT systems, leading to a better understanding of underlying concepts and practical skills that can be used in real-life situations. Secondly, the application of the IoTA-SRM framework in the micro-mobility use-case (as seen in Appendix A) dem-

onstrated its applicability in a real-world scenario. It was interesting to note that students who worked in different teams produced reports with similar structure, content, and analysis, thus highlighting the repeatability of results using the framework. The IoTA-SRM framework provided a structured and standardized approach to security analysis, leading to consistent and reliable results across different teams. Overall, applying the IoTA-SRM framework in the cybersecurity course highlighted its usefulness in guiding students towards desired outcomes and applicable to real-world scenarios, producing consistent and repeatable results.

The study also revealed several important lessons for designing and implementing effective hackathon learning models. One key lesson is the need for a careful balance in the number of lectures and resources provided to prevent information overload. It is also recommended to provide offline availability of lectures and materials for self-paced learning. Feedback served different purposes, with written feedback being more detailed, online consultation feedback providing the opportunity to answer questions, and presentation feedback offering peer and mentor support. It is advisable to introduce consultation and written feedback interactions with students at every hackathon event to provide ample opportunity for learning-oriented support. Clear and reviewed hackathon tasks are also important to ensure student-mentor interactions focus on learning-oriented activities. The interplay between lecture and feedback interventions benefited the student's learning process, highlighting the importance of making these interventions a staple and foundational part of the hackathon learning model to support learning. Overall, these findings underscore the value of introducing interventions to enrich hackathons and provide great support for learning about IoT security risk management.

7. Discussion

The research developed the IoTA-SRM framework for managing IoT security risks (answering **RQ1**) and proposed a hackathon learning model to encourage its application and promote learning about security risk management (answering **RQ2**), evaluating our findings in Section 6 (**RQ1**, **RQ2**). In this section, we discuss the implications of our findings to research and the limitations of the work.

7.1. *IoTA-SRM Framework*

The IoTA-SRM framework (see Section 4) addresses the limitations of existing security risk management approaches in IoT systems. Compared to related works, IoTA-SRM considers the unique characteristics of IoT systems and provides a systematic process for managing risks at multiple architectural layers. The framework adopts an architecture perspective, enabling a comprehensive asset-oriented system analysis, multi-layer risk impact analysis, risk treatment, and tradeoff analysis. We illustrated

Table 6
Comparison of IoT Security Risk Management Frameworks

Framework	Main Focus	Asset oriented	Architecture Perspective	Risk Management
IoTA-SRM (Our framework)	IoT security risk management	[++]	[++]	[++]
SecIoT (Huang *et al.*, 2016)	IoT security requirements, authentication, secure communications, authorisation, risk indicators	[++]	[+]	[+−]
COBIT5 (Latifi and Zarrabi, 2017)	IT risk management	[++]	[+]	[−]
IoT-HarPSecA (Samaila *et al.*, 2019)	Secure IoT design and implementation	[−]	[−]	[−]

[++] Mostly fulfilled, [+−] Fulfilled with limitations, [+] Partially explored, [−] Not fulfilled

our framework using the three-layer IoT architecture, but our framework can also be applied to any IoT architecture similarly decomposed into layers. The SecIoT framework proposed by Huang *et al.* (2016) covers IoT security requirements, authentication, secure communications, authorisation, and risk indicators. However, it did not recognise the architecture perspective of risk management or explore it systematically. Our framework extends the SecIoT framework by introducing the architecture perspective and performing a systematic security risk management analysis. Other related works, such as COBIT5 (Latifi and Zarrabi, 2017) and IoT-HarPSecA (Samaila *et al.*, 2019), discuss security concepts for IoT security risk management but do not provide a systematic approach to applying them. COBIT5 is a framework for IT risk management that can be applied to IoT risk management, but its application to IoT risk management was not explored systematically. IoT-HarPSecA is a security framework that facilitates secure IoT design and implementation through security requirements elicitation and cryptographic algorithms recommendation, but it did not explore security risk management analysis.

However, our framework can benefit from the best practices and references from related works (Huang *et al.*, 2016; Samaila *et al.*, 2019; Latifi and Zarrabi, 2017), covering asset management, risk assessment, risk management strategy, governance, etc., to perform a comprehensive and systematic security risk management analysis for IoT systems.

7.2. *Hackathon Learning Model*

Our hackathon approach supports applying the IoT security risk management framework (see Section 5), showing how hackathons can foster learning about IoT security risk management (see Section 6) to answer **RQ2**. Our approach differs from previous research that used hackathons for different purposes, such as developing prototypes or

promoting entrepreneurship, by utilizing hackathons as a teaching strategy to help students in the cybersecurity course gain practical knowledge of security risk management. Our approach also differs from related works using hackathons for learning in educational settings, integrating multiple hackathon events within the course, and providing students with ample learning opportunities.

Our findings on applying the hackathon learning model and its interventions indicate that our approach provided learning opportunities for the students as they progressed through the hackathon events and cybersecurity course. The lecture interventions provided rich content to aid student reflection on the IoT use case and to attempt the hackathon tasks. Rarely do papers discuss or highlight the benefits of carefully planned lectures at hackathon events to achieve learning outcomes. Our findings contribute to exploring the role of hackathon-influenced lecture interventions in the students' learning. In contrast, the feedback interventions promoted learning-oriented mentoring and guidance at multiple points of each hackathon event. Our hackathon method utilized mentor feedback as an intervention in written form, online consultation, and feedback at presentation sessions. Similarly, our findings align with previous research that highlighted the benefits of mentor support to aid students dealing with the complexities of their projects, provide the technical expertise necessary to complete projects and achieve desired learning outcomes (Nolte *et al.*, 2020a). We also see the learning benefits of including and facilitating peer-led feedback intervention, as explored by (Rukmono and Chaudron, 2022).

7.3. *Related Works*

We integrated the hackathon learning model into a cybersecurity course where students can apply the IoTA-SRM framework, and we assessed the learning benefits of this approach. Our approach shares some similarities with the related works, particularly in using hackathons and practical-oriented learning to teach cybersecurity. However, our approach differs from previous research, specifically focusing on teaching IoT security risk management through our framework and incorporating hackathon interventions.

Affia *et al.* (2022) integrated hackathons into a cybersecurity course to promote teamwork and learning about security. Similarly, our study implemented hackathon interventions, but we focused on teaching IoT security risk management through our framework at each hackathon event. Our findings align with Affia *et al.* (2022) and demonstrate that hackathon interventions can facilitate security learning.

Another related work is the competition-based hackathon organized by Cheung *et al.* (2011), which provided a practical cybersecurity scenario for students to apply their knowledge while working together in a high-pressure environment. However, their approach relies heavily on self-study and peer instruction efforts, which may disadvantage students who lack the motivation to learn independently. In contrast, our study found

Table 7
Related Work

Criteria	Affia *et al.* (2022)	Cheung *et al.* (2011)	Karagiannis and Magkos (2020)	OConnor and Stricklan (2021)	This paper
Security learning focus (i.e., security risk management)	+–	+	+	+	++
Hackathon for learning	+	+	+	+	+
Thematic input interventions	+	+–	+	+	+
Feedback interventions	+	+	–	–	+
Multiple hackathon iterations	+	–	+–	–	++

[++] Mostly fulfilled, [+] Partially fulfilled, [+–] Fulfilled with limitations, [–] Not fulfilled

that introducing lectures alongside hackathon interventions stimulated learning and encouraged self-study through online lecture recordings.

In Karagiannis and Magkos (2020), capture-the-flag (CTF) challenges were used to help undergraduate students acquire cybersecurity skills and knowledge. The approach incorporated gamification and self-directed and collaborative learning elements, encouraging teamwork and knowledge-sharing. Our study used hackathons to teach security risk management without relying on pre-existing cybersecurity skills. Our selected use-case and hackathon tasks provided practical-oriented learning and allowed students to adopt an adversarial thinking approach to security risk analysis from a hacker's perspective.

Finally, OConnor and Stricklan (2021) explored the benefits of gamification in a hands-on mobile and wireless cybersecurity course. The authors provided lectures and lab sessions, followed by a hackathon where students could demonstrate their knowledge of hacking wireless protocols. Our study similarly found benefits in introducing adversarial thinking through hackathons, but our interventions were more frequent and spread out, keeping students engaged throughout the learning process.

While most existing cybersecurity hackathon approaches focus on CTF and competition -based hackathons (Li and Kulkarni, 2016), our study provides a unique perspective on the application and suitability of hackathons for teaching security risk management (**RQ2**).

7.4. *Limitations*

Our study presented the IoTA-SRM framework for managing IoT security risks and a hackathon learning model to facilitate learning about IoT security risk management through an iterative learning-by-doing approach. The hackathon interventions were introduced as the driving force for learning, and the approach was analyzed in a cybersecurity course. While our study provides insights into the framework and the suitability and benefits of hackathon interventions for learning about IoT security risk management, some limitations to our work should be considered.

First, our findings cannot be generalized beyond the specific context of our course. It is possible that a different study conducted on a different course could produce different results. Second, the sample size of our study may be biased. However, we selected a cross-section of student teams that met specific criteria, such as team size and questionnaire response completeness, covering 62.5% of the students who attended and completed the cybersecurity course. This helped to mitigate the potential bias. Third, two out of three researchers were involved in planning, executing, and grading the hackathon events and the course, which could introduce bias to the reported findings. However, one researcher had no involvement in the hackathon's execution and refrained from interfering during the hackathon and the course until the data analysis commenced. Moreover, the post-hackathon questionnaire for all three hackathon events was not anonymous, which could also introduce bias to the reported results. However, we analyzed the data collected at the hackathon events only after the cybersecurity course was completed to avoid bias in grading the students in our data sample based on how they reacted to our intervention style. Finally, there may be some bias in reporting and analyzing the open-ended questions; however, we did not generalize or conclude from the responses but used them as potential explanations for our findings. Additionally, we avoided making causal claims in our analysis and provided a detailed description of the students' reported perceptions.

8. Concluding Remarks

Our study contributes to closing the gap between theory and practice in cybersecurity by developing a practical approach to learning and applying IoT security risk management concepts. We addressed this gap by first developing a framework for managing IoT security risks that decompose IoT system assets into architectural layers, perform a multi-layer risk analysis, and handle discovered risks (**RQ1**). We then proposed a hackathon approach to encourage the application of our proposed framework for IoT security risk management and promote learning about security risk management (**RQ2**). The findings of our action research, evaluating the framework and hackathon learning model, suggest that the hackathon model and its interventions benefit students' learning gains in IoT security management. However, future work is necessary to explore the benefits of hackathons in different educational settings, evaluate different types of interventions within the hackathon model, and implement methods to measure actual learning gains. Our findings also show that the IoTA-SRM framework is beneficial in guiding students towards desired learning outcomes, applicable to real-world scenarios, and producing consistent and repeatable results. Future work can explore extending the proposed framework to manage security risks in specific IoT applications or domains. Ultimately, this study provides valuable insights into effective teaching and learning approaches for IoT security risk management and contributes to the ongoing efforts to improve IoT security.

References

Affia, A.-a.O., Matulevičius, R., Nolte, A. (2019). Security risk management in cooperative intelligent transportation systems: A systematic literature review. In: *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pp. 282–300. Springer.

Affia, A.-a.O., Matulevičius, R., Tõnisson, R. (2021). Security risk estimation and management in autonomous driving vehicles. In: *International Conference on Advanced Information Systems Engineering*, pp. 11–19. Springer.

Affia, A.-a.O., Nolte, A., Matulevičius, R. (2020). Developing and evaluating a hackathon approach to Foster cyber security learning. In: *International Conference on Collaboration Technologies and Social Computing*, pp. 3–19. Springer.

Affia, A.-a.O., Nolte, A., Matulevičius, R. (2022). Integrating hackathons into an online cybersecurity course. In: *2022 IEEE/ACM 44th International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET)*, pp. 134–145. https://doi.org/10.1109/ICSE-SEET55299.2022. 9794183

Ali, B., Awad, A.I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *sensors*, 18(3), 817.

Angermeier, D., Nieding, A., Eichler, J. (2016). Supporting risk assessment with the systematic identification, merging, and validation of security goals. In: *International Workshop on Risk Assessment and Risk-driven Testing*, pp. 82–95. Springer.

Byrne, J.R., O'Sullivan, K., Sullivan, K. (2016). An IoT and wearable technology hackathon for promoting careers in computer science. *IEEE Transactions on Education*, 60(1), 50–58.

Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R. (2007). Introducing octave allegro: Improving the information security risk assessment process. Technical report, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

Cheung, R.S., Cohen, J.P., Lo, H.Z., Elia, F. (2011). Challenge based learning in cybersecurity education. In: *Proceedings of the International Conference on Security and Management (SAM)*, p. 1. Citeseer.

Crumpler, W., Lewis, J.A. (2019). The cybersecurity workforce gap. *Center for Strategic and International Studies (CSIS) Washington, DC, USA*.

Cvitić, I., Vujić, M., *et al.* (2015). Classification of security risks in the IoT environment. *Annals of DAAAM & Proceedings*, 26(1).

CWE (a). (2020). Common Weakness Enumeration. A community-developed dictionary of software weakness types. [Online]. Accessed: 2020-03-20.

Dubois, É., Heymans, P., Mayer, N., Matulevičius, R. (2010). A systematic approach to define the domain of information system security risk management. In: *Intentional Perspectives on Information Systems Engineering*. Springer, pp. 289–306.

Fagan, M., Marron, J., Brady Jr, K.G., Cuthill, B.B., Megas, K.N., Herold, R., Lemire, D., Hoehn, B. (2021). IoT device cybersecurity guidance for the Federal government. *NIST Special Publication*, 800, 213.

Fries, R., Chowdhury, M., Brummond, J. (2009). Transportation Infrastructure Security Utilizing Intelligent Transportation Systems.

Gama, K., Alencar Gonçalves, B., Alessio, P. (2018). Hackathons in the formal learning process. In: *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, pp. 248–253.

García-Hernández, A., González-Ramírez, T. (2018). Construction and validation of a questionnaire to assess student satisfaction with mathematics learning materials. In: *Proceedings of the Sixth International Conference on Technological Ecosystems for Enhancing Multiculturality*, pp. 134–138.

Gliem, J.A., Gliem, R.R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. In: Midwest Research-to-Practice Conference in Adult, Continuing, and Community.

Hamman, S.T., Hopkinson, K.M. (2016). Teaching adversarial thinking for cybersecurity. *Journal of the Colloquium for Information Systems Security Education*, 4, 19–19.

Huang, X., Craig, P., Lin, H., Yan, Z. (2016). SecIoT: a security framework for the Internet of Things. *Security and Communication Networks*, 9(16), 3083–3094.

Kam, H.-J., Katerattanakul, P. (2019). Enhancing student learning in cybersecurity education using an out-of-class learning approach. *Journal of Information Technology Education. Innovations in Practice*, 18, 29.

Kandasamy, K., Srinivas, S., Achuthan, K., Rangan, V.P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, 2020(1), 1–18.

Karagiannis, S., Magkos, E. (2020). Adapting CTF challenges into virtual cybersecurity learning environments. *Information & Computer Security*.

Kessler, G.C. (2012). Information security: New threats or familiar problems? *Computer*, 45(2), 59–65.

Kollwitz, C., Dinter, B. (2019). What the Hack?–Towards a Taxonomy of Hackathons. In: *International Conference on Business Process Management*, Springer, pp. 354–369.

Kumar, N.M., Mallick, P.K. (2018). The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. *Procedia Computer Science*, 132, 109–117.

Latifi, F., Zarrabi, H. (2017). A COBIT5 Framework for IoT risk management. *International Journal of Computer Applications*, 170(8), 40–43.

Lewin, K. (1946). Action research and minority problems. *Journal of social issues*, 2(4), 34–46.

Li, C., Kulkarni, R. (2016). Survey of cybersecurity education through gamification. In: *2016 ASEE Annual Conference & Exposition*.

Lombardi, M., Pascale, F., Santaniello, D. (2021). Internet of things: A general overview between architectures, protocols and applications. *Information*, 12(2), 87.

Malik, V., Singh, S. (2019). Security risk management in IoT environment. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(4), 697–709.

Matulevičius, R. (2017). *Fundamentals of Secure System Modelling*.

Mayer, N. (2009). *Model-based Management of Information System Security Risk*. PhD thesis, University of Namur.

NIST, N. (2002). Risk management guide for information technology systems. *NIST Special Publication*, 800(30), 800–30.

Nolte, A., Hayden, L.B., Herbsleb, J.D. (2020a). How to support newcomers in scientific hackathons – An action research study on expert mentoring. In: *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW1), 25–202023.

Nolte, A., Pe-Than, E.P.P., Affia, A.-a.O., Chaihirunkarn, C., Filippova, A., Kalyanasundaram, A., Angarita, M.A.M., Trainer, E., Herbsleb, J.D. (2020b). How to organize a hackathon – A planning kit. *arXiv preprint arXiv:2008.08025*.

NVD (a). (2019). *National Vulnerability Database*. National Institute of Standards and Technology. [Online]. Accessed: 2019-05-30.

OConnor, T., Stricklan, C. (2021). Teaching a hands-on mobile and wireless cybersecurity course. In: *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 1*, pp. 296–302.

OWASP (2021). OWASP Top 10:2021. Available at `https://owasp.org/Top10/`

Oyetade, K., Zuva, T., Harmse, A. (2022). Educational benefits of hackathon: A systematic literature review. *World Journal on Educational Technology: Current Issues*, 14, 1668–1684. `https://doi.org/10.18844/wjet.v14i6.7131`

Pe-Than, E.P.P., Nolte, A., Filippova, A., Bird, C., Scallen, S., Herbsleb, J.D. (2019). Designing corporate hackathons with a purpose: The future of software development. *IEEE Software*, 36(1), 15–22.

Resul, D., Gündüz, M.Z. (2020). Analysis of cyber-attacks in IoT-based critical infrastructures. *International Journal of Information Security Science*, 8(4), 122–133.

Rukmono, S.A., Chaudron, M.R. (2022). Guiding Peer-feedback in Learning Software Design using UML.

Samaila, M.G., José, M.Z., Sequeiros, J.B., Freire, M.M., Inácio, P.R. (2019). IoT-HarPSecA: A framework for facilitating the design and development of secure IoT devices. In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1–7.

Sauro, J. (2011). MeasuringU: Measuring Usefulness. *Measuringu. com*.

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, 44, 100467.

Shostack, A. (2014). *Threat Modeling: Designing for Security*. John Wiley & Sons, 9781118809990.

Swamy, S.N., Kota, S.R. (2020). An empirical study on system level aspects of Internet of Things (IoT). *IEEE Access*, 8, 188082–188134.

Wang, P., Sbeit, R. (2020). A comprehensive mentoring model for cybersecurity education. In: *17th International Conference on Information Technology–New Generations (ITNG 2020)*, Springer, pp. 17–23.

Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J., Du, H.-Y. (2010). Research on the architecture of Internet of Things. In: *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)* (Vol. 5). IEEE, pp. 5–484.

Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., Graubart, R., Clausen, L. (2011). *Threat Assessment & Remediation Analysis (TARA): Methodology Description Version 1.0*. Technical report, MITRE CORP BEDFORD MA.

A.-a.O. Affia is a junior research fellow and a final year doctoral student of Computer Science at the University of Tartu, Estonia. She received her Master's degree in Cybersecurity from Tallinn University of Technology and the University of Tartu, Estonia. Her research interests include the security of information systems and intelligent infrastructure systems, and security risk management in intelligent infrastructure systems. Additionally, her work has focused on developing and implementing hackathon-based learning models that enable participants to understand better complex security risk management processes for intelligent infrastructure systems.

A. Nolte is an Associate Professor at the University of Tartu (Estonia) and an Adjunct Associate Professor at Carnegie Mellon University (Pittsburgh, PA, USA). He holds a master's degree in computer science from TU Dortmund University (Germany) and a PhD in information systems from the University of Duisburg-Essen (Germany). His research focuses on understanding and developing means to support collaboration in corporate, entrepreneurial, civic, educational, and scientific settings. He has published more than 100 research papers and articles in top conferences and journals in the fields of human-computer interaction, information systems, and software engineering. His research has received multiple awards, including an ACM SIGSOFT Distinguished Paper Award.

R. Matulevičius is a Professor of information security at the University of Tartu, Estonia. His publication record includes over 100 articles published in peer-reviewed journals, conferences, and workshops. He is the author of the book Fundamentals of Secure System Modelling (Springer, 2017). His research interests include information security and privacy, security risk management, security and privacy by design and model-driven security in intelligent infrastructure, blockchain and information systems. He has been involved in the SPARTA H2020 project, Erasmus+ Strategic Partnership programs CyberPhish, BlockNet and BLISS. Currently, R. Matulevičius is the principal researcher in CHESS (EU Horizon Europe) and CHAISE (Erasmus+ Sector Skills Alliances program) projects.

A.
Appendix A: Scooter Ride-Hailing System IoT Use-case

The system provides micro-mobility services consisting of different components: Scooter (**S**), Scooter Backend (**SB**), Scooter Mobile Application (**SMA**), and Rider (**R**). *The description below provides a general overview of a scooter ride-hailing system and, thus, is not an exhaustive explanation of the system-component interaction. You are allowed to assume the existence of lower-level components not explicitly mentioned in the case but are vital to any working software system.*

- **Scooter (S)**: The scooter component of the system is used to fulfill commutes. The scooter chassis (external hardware) houses its wheels, lights, batteries, cables, and connectors. Inside its chassis, the scooter contains various perception (i.e., sensing, positioning, actuating), network, and application (i.e., storage) assets. Below are the important assets classified by their information processing functions.
- **Scooter Backend (SB)**: Scooter backend is comprised of systems that help to monitor the status and location of a fleet of scooters, send commands to the scooter to lock/unlock, manage the user accounts and scooter ride activities. The **SB** can only be accessed through an administrative web interface.
- **Scooter Mobile Application (SMA)**: The scooter mobile application comes in Android and iOS implementations comprising the rider profile, ride-hailing, and billing components.
- **Rider (R)**: A rider is a user registered on the system and possesses a valid and active account. A rider should have access to the system's scooter (**S**) services and cannot use more than one S at a time.

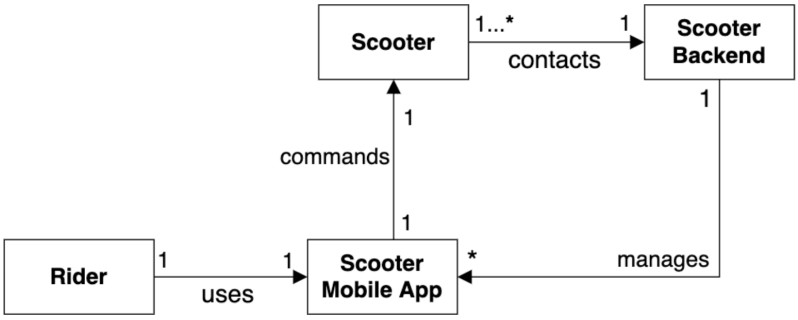

Fig. 11. Scooter Ride-Hailing System IoT use-case.

B.
Appendix B

Table 8

Post-Hackathon Questionnaire Instrument

Perception of the usefulness of the interventions (based on Sauro (2011)) anchored between strongly disagree and strongly agree.

Using the [*intervention*] enabled me to accomplish tasks more quickly.
Using the [*intervention*] improved my team's performance.
Using the [*intervention*] increased my productivity in the hackathon.
Using the [*intervention*] enhanced my effectiveness in my team.
Using the [*intervention*] made it easier to complete my *[hackathon]* solution.
I found the [*intervention*] useful in my team.

Perception of the level of agreement about students' evaluation of the intervention at the hackathon event (based on Garcķa-Hernįndez and Gonzįlez-Ramķrez (2018)), anchored between strongly disagree and strongly agree.

The [*intervention*] enhanced my satisfaction with the study of [*hackathon*] activity.
The [*intervention*] contributed to better learning of [*hackathon*] activity .
The [*intervention*] were easy to understand and connected to my learning interests.
The [*intervention*] made me forget how difficult the [*hackathon*] activity is.

Perception of the level of agreement about the interventions' contribution to learning at the hackathon event (based on Garcķa-Hernįndez and Gonzįlez-Ramķrez (2018)) anchored between strongly disagree and strongly agree.

The [*intervention*] linked its contents with my security interests.
The [*intervention*] made visible the linking of the [*hackathon*] activity with the real world.
The [*intervention*] was adapted to my learning rhythm.

Learning outcome measured students' perception of the hackathon learning process (based on Affia *et al.* (2022)) anchored between strongly disagree and strongly agree.

The hackathons case study resembled a real-life situation.
The hackathons facilitated independent problem-solving.
The hackathons allowed me the opportunity to design secure systems and software.
The hackathon activities made my learning experience more productive.
The hackathons provided enough opportunities during the course to find out if I clearly understood the course material.

Open ended questions.

Is there anything else you want to tell us about your [*intervention*] experience?
Is there anything else you want to tell us about your overall learning experience?