# RAM-IoT: Risk Assessment Model for IoT-Based Critical Assets

Kayode S. Adewole[1,2][a], Andreas Jacobsson[1,2][b] and Paul Davidsson[1,2][c]
[1]*Department of Computer Science and Media Technology, Malmö University, Malmö, Sweden*
[2]*Internet of Things and People Research Center, Malmö University, Malmö, Sweden*
{*kayode.adewole, andreas.jacobsson, paul.davidsson*}*@mau.se*

Keywords: Internet of Things, Risk Assessment, Threat, Vulnerability, Fuzzy AHP, Security and Privacy.

Abstract: As the number of Internet of Things (IoT) devices continues to grow, understanding and mitigating potential vulnerabilities and threats is crucial. With IoT devices becoming ubiquitous in critical sectors like healthcare, transportation, energy, and industrial automation, identifying and addressing risks is increasingly important. A comprehensive risk management approach enables IoT stakeholders to safeguard user data and privacy, as well as system integrity. Existing risk assessment frameworks focus on qualitative risk analysis methodologies, such as operationally critical threat, asset, and vulnerability evaluation (OCTAVE). However, security risk assessment, particularly for IoT ecosystem, demands both qualitative and quantitative risk assessment. This paper proposes RAM-IoT, a risk assessment model for IoT-based critical assets that integrates qualitative and quantitative risk assessment approaches. A multi-criteria decision making (MCDM) approach based on fuzzy Analytic Hierarchy Process (fuzzy AHP) is proposed to address the subjective assessment of the IoT risk analysts and their corresponding stakeholders. The applicability of the proposed model is illustrated through a use case connected to service delivery in the IoT. The proposed model provides a guideline to researchers and practitioners on how to quantify the risks targeting assets in IoT, thereby providing adequate support for protecting IoT ecosystems.

## 1 INTRODUCTION

The Internet of Things (IoT) has revolutionized how enterprises operate and do business. The IoT enables a network of interconnected machines and devices such as embedded computers, sensors, actuators, radio frequency identification (RFID), gateways, and remote servers to communicate and collaborate. This inter-connectivity drives significant process innovations, applications and a range of services including smart buildings, smart homes, smart agriculture, smart healthcare, intelligent transport systems, among others (Lee, 2020). The deployment of the IoT entails several technologies like wireless sensor networks, RFID, near field communication, wireless fidelity (WiFi), Bluetooth, and Internet protocols, paving ways for the collection of users' data and for transmission over the Internet (Jacobsson and Davidsson, 2015; Ali and Awad, 2018).

The IoT has enabled companies to collect huge quantities of personal information about their customers. The company with the most information about its customers and potential customers is typically regarded as the most successful company. Thus, personal information is the new oil for companies and fierce data collection is, to a large extent, made possible through the deployment of the IoT. However, the proliferation of IoT systems and technologies have also exposed companies and individuals to a growing number of cybersecurity attacks, leading to serious challenges for both persons and organizations in terms of risk for loss in reputation, compliance, financial stability, and business continuity, as well as to privacy exposures. This surge in cyberattacks is largely attributed to the rapid expansion of IoT devices in critical sectors such as smart buildings, smart grids, environmental monitoring, hospital patient care systems, smart manufacturing, and transport logistics, where security threats and vulnerabilities can have far-reaching consequences.

Nevertheless, the security and privacy risks associated with data collection and distribution in IoT ecosystem are of greater concerns (Amanullah et al., 2020; Adewole and Torra, 2022; Jacobsson and Davidsson, 2015; Adewole and Jacobsson, 2024a). There is a lack of effective IoT cyber risk manage-

[a] https://orcid.org/0000-0002-0155-7949
[b] https://orcid.org/0000-0002-8512-2976
[c] https://orcid.org/0000-0003-0998-6585



Adewole, K. S., Jacobsson, A. and Davidsson, P.
RAM-IoT: Risk Assessment Model for IoT-Based Critical Assets.
DOI: 10.5220/0013200800003944

In *Proceedings of the 10th International Conference on Internet of Things, Big Data and Security (IoTBDS 2025)*, pages 191-198
ISBN: 978-989-758-750-4; ISSN: 2184-4976

ment frameworks for managers (Lee, 2020; Ullah et al., 2021). Understanding the risks related to the use and possible misuse of information generated in IoT ecosystems and of those that target critical assets (e.g. hardware, software, sensors, data, etc) demands several efforts. This requires considerable analysis of different vulnerabilities, threats and risks, as explained by (Jacobsson and Davidsson, 2015). For the sake of clarity, an asset refers to any device, component, or resource that is part of the IoT ecosystem and contributes to its operation.

Risk assessment has long been identified as an important process to safeguard information systems and provide suitable mitigation strategies. Since the IoT is a technology that is based on Internet connectivity, it provides the same types of opportunities and risks as can be commonly found on the open Internet. In other words, IoT is susceptible to security vulnerabilities and is highly vulnerable to threats that may arise both within and outside those environments. Risk assessment processes have been characterized with high levels of uncertainty and imprecision (Abdel-Basset et al., 2019), demanding for risk assessment methodologies that incorporate both the subjective and objective analysis of risk assessment experts. Existing risk assessment approaches for IoT assets have focused mainly on qualitative risk assessment models (Ali and Awad, 2018; Ullah et al., 2021) such as operationally critical threat, asset, and vulnerability evaluation (OCTAVE) (Ali and Awad, 2018), ISO/IEC 27005 Information Security Risk Management (ISO/IEC, 2024), and the NIST SP 800-30 Risk Management Framework (NIST, 2024). Therefore, a model that integrates both qualitative and quantitative risk assessment of IoT critical assets is urgently needed. This is the goal of the proposed RAM-IoT – a risk assessment model for IoT-based critical assets. The proposed model also incorporates the opinion of the experts during the risk assessment process. By doing so, this paper contributes in the following ways:

- proposes a model that assesses the risks targeting assets in IoT ecosystems based on different types of service delivery,
- provides a risk assessment model that integrates both qualitative and quantitative risk assessment methods to accommodate the opinions of IoT risk assessment experts during the analysis process,
- investigates fuzzy Analytic Hierarchy Process (fuzzy AHP) for assessing risks in the IoT due to the high levels of uncertainty in risk assessment processes, and
- presents a use case scenario to demonstrate the usefulness of the proposed risk assessment model.

The remaining part of this paper is organized as follows. In Section 2, we discuss related works in the domain of risk assessment in IoT-based ecosystem. Section 3 presents a detailed description and discussion on the RAM-IoT. In Section 4, we present a use case scenario to highlight the applicability of the proposed risk assessment model, and finally, Section 5 concludes the paper and discusses future research areas.

## 2 RELATED WORK

The literature on risk assessment has for the most part focused on two distinct dimensions: qualitative and quantitative risk assessment. Typically, qualitative approaches provide subjective assessment to risk management while quantitative approaches focus on objective analysis based on numerical measures. Some well-known qualitative risk management frameworks include ISO/IEC 27005 (ISO/IEC, 2024), NIST SP 800-30 (NIST, 2024), OCTAVE (ENISA, 2024), and OCTAVE Allegro (Caralli et al., 2007). The ISO/IEC 27005 deals with a set of standards developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The main purpose is to provide support for managers on how to manage information security risks. Although ISO/IEC 27005 provides some guidelines on sequence of activities, the framework does not directly employ any specific risk management method. Therefore, organization will have to define its own approach for risk management method based on its specific needs. NIST cybersecurity framework also provides five functions centred to organizational risk management. None of these frameworks explicitly address risk assessment of assets in IoT ecosystems.

Ali et al. (Ali and Awad, 2018) propose a qualitative risk assessment for IoT-systems based on the OCTAVE methodology. The authors highlights the threats and risks connected to IoT-based systems, as well as the importance of proper mitigation strategies to reduce such risks.

A systematic literature review that covers 796 articles with 56 risks related to the IoT has been proposed in (Ullah et al., 2021). The authors further proposed a multilayered structural division of risk management for smart cities governance based on technology, organisation, environment (the TOE framework) . The authors employed metrics such as category score, overall score, category rank, and overall rank to determine the criticality of the identified risks with respect to each layer in TOE. Lee et al.

(Lee, 2020) present a review of IoT cybersecurity risk management frameworks that cover both qualitative and quantitative approaches, and in their review, they also propose a four-layered IoT cyber risk management framework consisting of (1) IoT cyber ecosystem layer, (2) IoT cyber infrastructure layer, (3) IoT cyber risk assessment layer, and (4) IoT cyber performance layer.

Khosravi-Farmad et al. (Khosravi-Farmad and Ghaemi-Bafghi, 2020) proposed a quantitative risk management approach that is based on Bayesian decision networks. The framework also expands Bayesian attack graphs by integrating risk mitigation phases to address countermeasures for risk reduction. The proposed model is made up of three phases: (1) risk assessment, (2) risk mitigation, and (3) risk validation and monitoring. One possible improvement of their proposed approach is the need to improve the accuracy of the risk assessment process.

A quantitative risk assessment model that is especially related to privacy in smart homes IoT-based systems is presented in (Werner et al., 2022). A questionnaire covering 15 major concerns with respect to privacy were designed to reveal several features of the connected home IoT devices for the purpose of assessing the risks that are targeting them. Similarly, (Wang et al., 2023) proposed a privacy risk assessment method called STPA–FMEA to uncover 35 privacy risk scenarios related to smart home systems.

While there are many risk assessment frameworks in the literature, none of them, to the best of our knowledge, fully integrates qualitative and quantitative approaches to provide an enhanced method for the analysis and management of risk in IoT ecosystems. In addition, these studies typically also pay less attention to risk assessment methodology that takes into consideration aspects of uncertainty in their risk measurement approaches. In this paper, we aim to fill these gaps by proposing a model that explicitly integrates the opinions of IoT experts, researchers, practitioners, and risk analysts during the risk assessment process, while also incorporating fuzzy AHP to that aspects of uncertainty and imprecision that are associated with risk assessment. Our proposed method, RAM-IoT, thus integrates both qualitative and quantitative approaches, while also taking uncertainty into account, specifically for risk assessment in the IoT.

# 3 PROPOSED APPROACH

This section details the components of RAM-IoT and provides formal guidance on its requirements. RAM-IoT is an asset-based risk assessment model designed for IoT ecosystems, considering the various layers involved in the typical case of IoT service delivery. Each layer introduces specific attack surfaces that may be exposed through interactions between components across different layers. The model acknowledges the inherently subjective nature of risk assessments conducted by IoT analysts and other stakeholders. To address this, RAM-IoT employs both qualitative and quantitative risk assessment methods, offering a comprehensive and robust approach to risk assessment and mitigation within IoT ecosystems.

As shown in Figure 1, the proposed risk assessment model consists of different modules. RAM-IoT considers fuzzy AHP as a multi-criteria decision making (MCDM) approach for risk assessment to define empirical risk measures relating to the vulnerabilities and threats targeting the specific asset. Therefore, the model can be viewed as providing a set of formal structural guidelines to IoT risk analysts and their corresponding stakeholders on how to identify and quantify risks that are associated with specific assets in the IoT.

RAM-IoT can be formally conceptualized as a tuple $IE = (U, S, A, V, T, R, F)$ where $IE$: the IoT ecosystem, $U$: users, $A$: assets related to $S$, $S$: IoT services, $V$: vulnerabilities related to the assets which can be exploited by threat sources, $T$: threats targeting the assets $A$, $R$: risks estimation function that addresses both qualitative and quantitative risk assessment methodologies. $F$: a mapping function that maps the risk score to risk severity. The detail of each component is provided as follows.

## 3.1 The IoT Ecosystem (*ie*)

Figure 2 presents a generic four-layer architecture of IoT highlighting security and privacy as major concerns. The security and privacy issues cut across the different layers of the IoT ecosystem including the perception where the ”things” (devices, actuators, etc.) in the IoT are accommodated. The network layer that concerns with communication technologies, such as Zigbee, WiFi, Bluetooth, Celullar (e.g. 5G), LoRaWAN, and MQTT (Adewole and Jacobsson, 2024a; Adewole and Jacobsson, 2024b). The management layer that is responsible for storage, computing and device management, as well as for the application and service layer that accommodates different software applications that render services to the users. Services may include support for building automation, health and wellness, energy consumption monitoring, safety and security surveillance, and so on. Users interact with various components in the IoT ecosystem, hence, their security and privacy are of

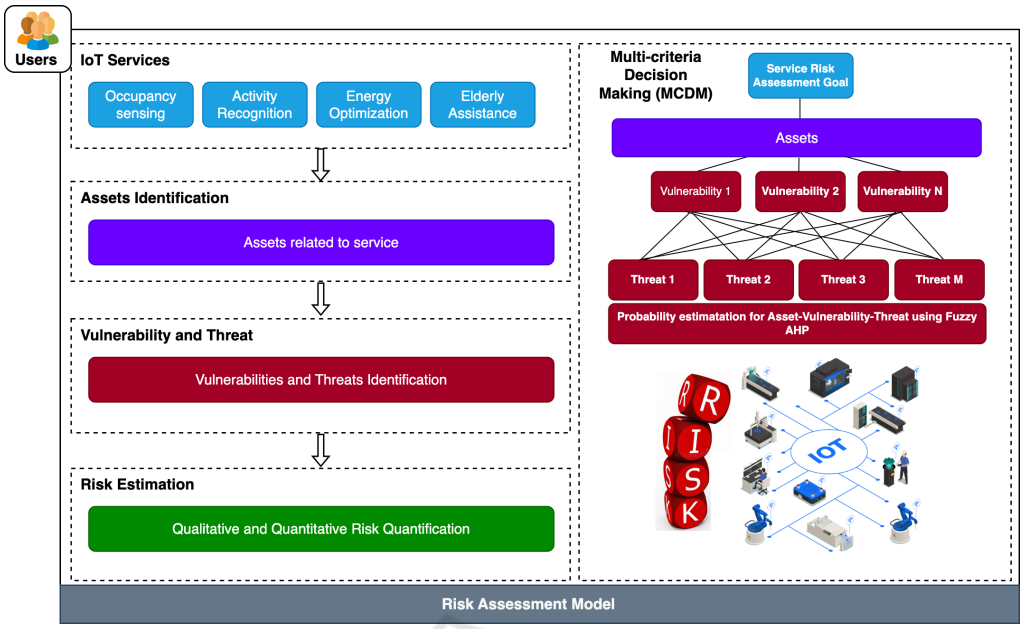


Figure 1: Proposed asset-based risk assessment model for IoT.

major concern. Thus, risk assessment of assets used in the ecosystems is important and beneficial to the IoT stakeholders.

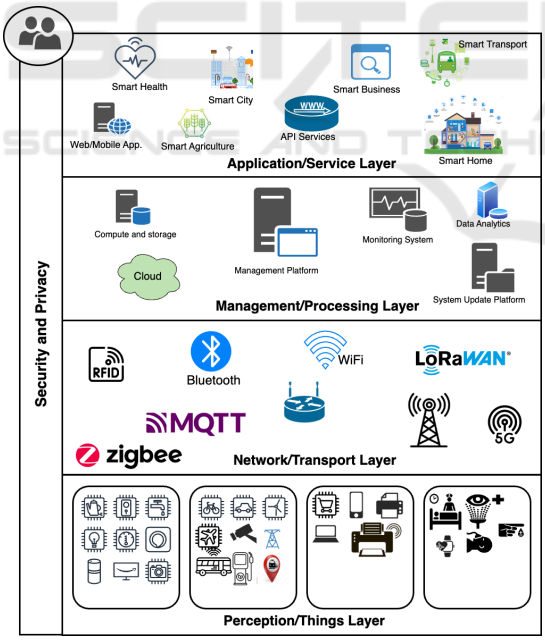


Figure 2: A four-layered IoT reference architecture.

## 3.2 Users ($U$)

Users interact with $IE$ through a specific IoT service, typically through a smartphone. For instance, an occupancy detection system may requires occupancy sensor that keeps track of user presence or absence in a room. A set of users is denoted as $U_{i=1}^{m} = \{u_1, u_2, ..., u_m\}$, $\forall u_i \in U$. We assume $m$ is dynamic, because a user $u_i$ can join or leave the network at any time.

## 3.3 IoT Services ($S$)

One of the benefits of the IoT is service delivery to users. Every activity or behavior of a user $u_i \in U$ signifies a specific service $s_i \in S$, where $S$ is denoted as a set of IoT services or applications, i.e., $S = \{s_1, s_2, ..., s_j\}$. Typical services or applications include occupancy detection, activity recognition, fire detection, and security surveillance, among others.

## 3.4 Assets ($A$)

In the context of the IoT, an asset refers to any device, component, or resource that is part of the IoT ecosystem and contributes to its operation. RAM-IoT viewed assets as the nodes $N$ in the IoT ecosystem that have the capability to sense, actuate, process, and transmit data. Assets can also denote the data $D$ being transmitted or the communication links $C$ between different nodes (i.e., smart devices). The goal of a malicious agent is to target a specific asset. Thus, they serve as the major reason for risk assessment.

We identify $A = \{N \cup D \cup C_{nl \to nk}\}$, $N$ is the set of devices used by user $u_i$, $\forall u_i \in U$ such as smart camera, smartphone, laptop, edge servers, and gateways. Similarly, $D$ is the data originated from node $n, n \in N$.

$C_{nl \to nk}$ is the communication link between nodes $nl$ and $nk$. One possible strategy by malicious agent to compromise asset is through the communication network. For example, Distributed Denial-of-Service attacks (DDoS) is a category of IoT threats that targets communication links (Amanullah et al., 2020), rendering it unavailable to use for the intended IoT service.

## 3.5 Vulnerabilities ($V$) and Threats ($T$)

We defined $V$ as a set of vulnerabilities. Information about IoT vulnerabilities can be obtained using vulnerability scanning tools such Nessus or by searching the online vulnerability databases like MITRE's Common Vulnerabilities and Exposures (so called CVEs). Similarly, $T$ denotes a set of threats targeting assets $a, a \in A$. A threat is always triggered from one or more vulnerabilities $v, v \in V$. For example, unauthorized information leakage is a threat that can exploit weak data protection mechanism vulnerability to compromise data asset when it flows through the IoT ecosystem. Therefore, the role of the IoT risk analyst is to identify the vulnerabilities and threats related to a specific asset when deployed in order to deliver IoT services. This is needed for the construction of the fuzzy pairwise comparison matrix for the subjective risk assessment part of RAM-IoT (see Algorithm 1).

## 3.6 Risk Functions ($R$)

To estimate the risk related to the assets to deliver service $s$, we defined two functions, $R_a(s)$ and $R(s)$. The former denotes the risk related to asset $a$ when used to deliver service $s$. The latter is the accumulated risks for delivering service $s$ based on the different assets. $R_a(s)$ is given as.

$$R_a(s) = \Theta_{a \in A}(a) * \max(\Omega_a(T,V), \Delta_{avt}(T,V)) \quad (1)$$

where $\Theta(a)$ is the cost function (risk impact) related to a specific asset used to deliver service $s$. $\Omega_a(T,V)$ and $\Delta_{avt}(T,V)$ are two probabilities (risk likelihoods) obtained from fuzzy AHP ranking. While $\Omega_a(T,V)$ is based on independent assessment of vulnerabilities and threats in relation to the asset, $\Delta_{avt}(T,V)$ considered asset-vulnerability-threat as dependent components. $\Theta_{a \in A}(a)$ is defined as.

$$\Theta_{a \in A}(a) = \sum_{i \in \{N,D,C\}} \theta(i) \quad (2)$$

In this case, Eq. 2 accumulates all the costs associated with asset $a$. Recall that $N, D, C \in A$ as previously defined. Therefore,

$$\Omega_a(T,V) = \max(P(V_a), P(T_a)) \quad (3)$$

where $P(V_a)$ and $P(T_a)$ are two independent probabilities computed from the ranks of fuzzy AHP. The motivation for using the max function stems from the fact that risk likelihood is measured as a probability. Eq. 4 and 5 give the computation of $P(V_a)$ and $P(T_a)$.

$$P(V_a) = \prod_{j=1}^{n} v_{aj} \quad (4)$$

$$P(T_a) = \prod_{j=1}^{m} t_{aj} \quad (5)$$

The probabilities $v_{aj}$ and $t_{aj}$ denote vulnerability and threat likelihoods at each layer of the MCDM (see Algorithm 1 and Figure 1). Formally, $\Delta_{avt}(T,V)$ is given as.

$$\Delta_{avt}(T,V) = \max_{k}(\delta_{avt_k}(T,V)) \quad (6)$$

where $\delta_{avt_k}(T,V)$ represents the leave node of the MCDM of the fuzzy AHP approach (i.e. the final weight of fuzzy AHP corresponding to individual asset-vulnerability-threat). Hence, the accumulated risks for delivering service $s$ based on the different assets is given in Eq. 7.

$$R(s) = \sum_{a=1}^{|A|} R_a(s) \quad (7)$$

### 3.6.1 Fuzzy AHP

In 1970, Saaty (Saaty and Vargas, 1979) proposed the idea of Analytic Hierarchy Process (AHP), which is an MCDM method for organizing and analyzing complex decisions in the present of many alternatives. MCDM such as AHP has been widely used in many fields including ranking, prioritizing, risk analysis, designing and planning, among others (Abdel-Basset et al., 2019). AHP has shown remarkable achievement for risk analysis in supply chains to determine a set of sustainable supplier selection criteria (Luthra et al., 2017; Abdel-Basset et al., 2019).

Nevertheless, AHP has a drawback as it cannot incorporate subjectivity or uncertainty in a decision making process (Abdel-Basset et al., 2019). Therefore, fuzzy AHP technique, which is related to fuzzy logic and MCDM, has been proposed as a replacement (see for example (Ramík and Korviny, 2010)). Table 1 compares fuzzy AHP intensity scale with Saaty scale. It can be seen that AHP is based on a nine-point scale that is used for assessing the relative importance of each pairs of criteria. The motivation for adopting fuzzy AHP is to address the subjective assessment of the IoT risk analysts and to integrate both qualitative and quantitative risk assessment methods in the proposed model.

During risk assessment, IoT risk analyst creates a fuzzy pairwise comparison matrix related to each vulnerability with respect to the target asset as well as the threats with respect to the vulnerabilities that could be triggered by the threat sources (see Figure 2 and Algorithm 1). This fuzzy comparison matrix is generally given as:

$$\tilde{A} = \begin{bmatrix} 1 & \tilde{a}_{12} & ... & \tilde{a}_{1n} \\ \tilde{a}_{21} & 1 & ... & \tilde{a}_{2n} \\ ... & ... & 1 & ... \\ \tilde{a}_{n1} & \tilde{a}_{n2} & ... & 1 \end{bmatrix} \quad (8)$$

where $\tilde{a}_{ij} = (1,1,1)$ if $i$ is equal to $j$ and $\tilde{a}_{ij} = \tilde{1}, \tilde{3}, \tilde{5}, \tilde{7}$ or $\tilde{1}^{-1}, \tilde{3}^{-1}, \tilde{5}^{-1}, \tilde{7}^{-1}, \tilde{9}^{-1}$ if $i$ is not equal to $j$.

Table 1: Fuzzy AHP scale with respect to Saaty scale.

| Intensity of Important | Fuzzy number | Description | Membership function | Reciprocal |
|---|---|---|---|---|
| 1 | $\tilde{1}$ | Equally important/preferred | (1,1,2) | (1/2,1,1) |
| 3 | $\tilde{3}$ | Moderately more important/preferred | (2,3,4) | (1/4,1/3,1/2) |
| 5 | $\tilde{5}$ | Strongly more important/preferred | (4,5,6) | (1/6,1/5,1/4) |
| 7 | $\tilde{7}$ | Very strongly more important/preferred | (6,7,8) | (1/8,1/7,1/6) |
| 9 | $\tilde{9}$ | Extremely more important/preferred | (8,9,10) | (1/10,1/9,1/8) |

In fuzzy AHP, each rank computed for vulnerabilities and threats need to be defuzzified to obtain the crisp values. For the fuzzy AHP part, we employed Ramik AHP as described in (Ramík and Korviny, 2010). Algorithm 1 provides a detailed description of RAM-IoT model for risk assessment.

### 3.7 Mapping Function ($F$)

The purpose of the mapping function $F$ is to establish the risk severity level for the risk score obtained from Algorithm 1. This severity level will assist IoT risk analysts and their stakeholders to make an informed decision regarding the risk of delivering the IoT service using the different identified assets. The first step is to normalize the risk score $R(s)$ to a value in the interval [0,1] using the Min-Max normalization. The IoT risk analyst then determine the Min and Max values based on expert knowledge. Min-Max normalization is given as:

$$R_{norm}(s) = \frac{R(s) - \min(R(s))}{\max(R(s)) - \min(R(s))} \quad (9)$$

Secondly, the normalized risk score is mapped by function $F$ to determine the risk severity level such that:

$$R_{sev} = F(R_{norm}(s)) \quad (10)$$

We then define a membership function for risk severity level $R_{sev}$ as in Eq. 11.

$$R_{sev} = \begin{cases} Low & \text{if } R_{norm}(s) < 0.5 \\ Medium & \text{if } 0.5 \leq R_{norm}(s) < 0.7 \\ High & \text{if } R_{norm}(s) \geq 0.7 \end{cases} \quad (11)$$

Algorithm 1: Proposed RAM-IoT.

**Input:** IoT service s, assets A
**Output:** risk score $R(s)$
Identify all assets $a \in B, B \in A$ needed to deliver service $s$
**while** $a \in B$ **do**
  Estimate asset costs (risk impact) according to Eq. 1 and 2
  Identify all vulnerabilities $v \in V$ and threats $t \in T$ targeting $a$
  Develop AHP MCDM hierarchy for risk modeling as shown in Figure 1
  Create the fuzzy comparison matrices according to Eq. 8 and Table 1
  Calculate the inconsistency index (NI) based on (Ramík and Korviny, 2010)
  Determine ranks/weights for each vulnerabilities and threats using Ramik Fuzzy AHP (Ramík and Korviny, 2010)
  Calculate risk likelihoods for $\Omega_a(T,V)$ and $\Delta_{avt}(T,V)$ using Eq. 3 and 6 based on the ranks/weights
  Compute the risk score $R_a(s)$ using Eq. 1
  Sum up the risk scores for $R(s)$ using $R_a(s)$ for asset $a$
**end**
Return $R(s)$

## 4 USE CASE

In this section, we present a use case scenario related to smart room booking service. A typical IoT-based room booking system in a smart building may be seen as a cross section of the IoT and thus includes the following components: IoT sensors such as smart IP camera to capture occupancy; a web/mobile booking platform that allows users to book rooms; smart door lock for access control to the room; a digital displays mounted outside the room to show real-time booking information, such as current reservations, availability, and upcoming schedules. A network and communication infrastructure that connects the IoT devices, sensors, and the booking platform, enabling seamless communication and data exchange across the system.

To keep the discussion simple, we present MCDM hierarchical structure that will be used for risk assessment as shown in Figure 3. This figure comprises three assets from the described scenario. Six vulnerabilities and threats were identified as shown in the figure. Next is to apply fuzzy AHP to compute the risk likelihoods as discussed in Section 3. For the fuzzy AHP part, we used the fuzzy AHP tool developed by Palacký University Olomouc (Palacký University Olomouc, 2024) since it is based on Ramik fuzzy AHP (Ramík and Korviny, 2010) adopted in Algorithm 1.

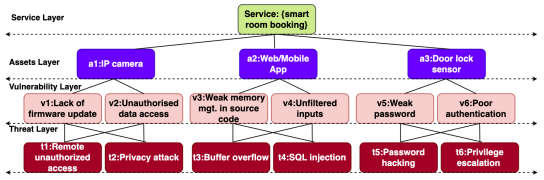


Figure 3: Use case scenario for smart room booking.

The fuzzy AHP pairwise comparison matrices are defined using this tool. We then obtain the respective risk likelihoods as discussed previously. Figure 4 shows a sample fuzzy comparison matrix for the vulnerabilities (i.e., lack of firmware update and unauthorized data access) with respect to the IP camera asset. We ranked lack of firmware update as strongly more important (i.e. (4,5,6)) than unauthorized data access (see Table 1). The reason is that if the firmware of the IP camera is well-secured, it could potentially prevent the threat to unauthorized data access. This shows a typical way in which fuzzy AHP can accommodate expert opinion in defining the pairwise comparison matrix. This process is repeated for other assets. The pairwise comparison matrix defined for the threat layer must be subjected to the vulnerability layer. This is how the ranking is performed until the final weights for asset-vulnerability-threat (i.e. the leave nodes) is obtained based on fuzzy AHP.

The results obtained for the sample use case is shown in Table 2. The descriptions of $a_1$ to $a_3$, $v_1$ to $v_6$, and $t_1$ to $t_6$ can be found in Figure 3.

From the results of the assets-based risk assessment approach demonstrated above, it can be seen that asset $a_2$ (i.e. Web/Mobile app) has the highest risk score based on the integration of qualitative and quantitative risk assessment methods. Furthermore, using Eq. 7, the overall risk score (i.e. $R(s)$) to deliver the smart room booking service is 142.72. Using expert knowledge, if we assume that the min and max values are 0 and 190 respectively, corresponding to no loss and the cost of losing all the assets, then, by Eq. 9, $R_{norm}(s)$ is 0.7511. Therefore, based on Eq. 11, the risk severity of delivering the service in the described

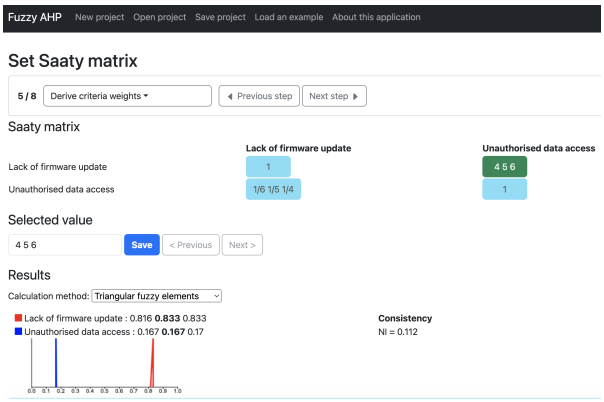


Figure 4: Sample comparison matrix for vulnerabilities with respect to IP camera asset.

Table 2: Results based on smart room booking use case.

| Asset ID | Asset | Vuln. | Threat | $\Theta(a)$ | $\Omega a$ | $\Delta_{avt}$ | $R_a(s)$ |
|---|---|---|---|---|---|---|---|
| 1 | a1 | v1 (0.833) v2 (0.167) $P(V_{a1}) =$ 0.139 | t1 (0.812) t2 (0.188) $P(T_{a1}) =$ 0.153 | $50 | 0.153 | 0.812 | 40.6 |
| 2 | a2 | v3 (0.250) v4 (0.750) $P(V_{a2}) =$ 0.188 | t3 (0.688) t4 (0.312) $P(T_{a2}) =$ 0.215 | $100 | 0.215 | 0.688 | 68.8 |
| 3 | a3 | v5 (0.833) v6 (0.167) $P(V_{a3}) =$ 0.139 | t5 (0.833) t6 (0.167) $P(T_{a3}) =$ 0.139 | $40 | 0.139 | 0.833 | 33.32 |

IoT environment (i.e. $IE$) with those vulnerabilities and threats is on the high side.

## 5 CONCLUSION

This paper presents a risk assessment model, RAM-IoT, that can be used to assess the risks relating to critical assets used for service delivery in IoT environments. To address the main gap identified in the literature, this study integrates both qualitative and quantitative risk assessment methods to provide a robust risk assessment approach. A multi-criteria decision making (MCDM) method that is based on fuzzy AHP was introduced to tackle the subjective assessment of IoT risk analysts. The proposed approach also addresses uncertainty and impreciseness in risk analysis. The model is useful for creating awareness of risks and to educate IoT stakeholders of the likelihood and scale of potential risks. RAM-IoT is envisioned as useful decision support in determining what actions are required to mitigate risks and their impacts

to IoT environments. In the future, we aim to automate the different components of the proposed model and to investigate the possibility of integrating it with the Common Vulnerability Scoring System (CVSS). It will also be interesting to study the applicability of the proposed model when considering risks that are related to human factor and context-specific risks.

## ACKNOWLEDGMENT

This work was partially funded by the Knowledge Foundation (Stiftelsen för kunskaps- och kompetensutveckling – KK-stiftelsen) via the Synergy project Intelligent and Trustworthy IoT Systems (Grant number 20220087).

## REFERENCES

Abdel-Basset, M., Gunasekaran, M., Mohamed, M., and Chilamkurti, N. (2019). A framework for risk assessment, management and evaluation: Economic tool for quantifying risks in supply chain. *Future Generation Computer Systems*, 90(1):489–502.

Adewole, K. S. and Jacobsson, A. (2024a). Homefus: A privacy and security-aware model for iot data fusion in smart connected homes. In *9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024)*, pages 133–140. Scitepress.

Adewole, K. S. and Jacobsson, A. (2024b). Lpm: A lightweight privacy-aware model for iot data fusion in smart connected homes. In *2024 9th International Conference on Smart and Sustainable Technologies (SpliTech)*, pages 1–7. IEEE.

Adewole, K. S. and Torra, V. (2022). Privacy issues in smart grid data: From energy disaggregation to disclosure risk. In *International Conference on Database and Expert Systems Applications*, pages 71–84. Springer.

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

Amanullah, M. A., Habeeb, R. A. A., Nasaruddin, F. H., Gani, A., Ahmed, E., Nainar, A. S. M., Akim, N. M., and Imran, M. (2020). Deep learning and big data technologies for iot security. *Computer Communications*, 151:495–517.

Caralli, R. A., Stevens, J. F., Young, L. R., and Wilson, W. R. (2007). Introducing octave allegro: Improving the information security risk assessment process. *Hansom AFB, MA*.

ENISA (2024). Octave v2.0 (and Octave-S v1.0 for Small and Medium Businesses) Product identity card. https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html. Accessed: 6th February, 2024.

ISO/IEC (2024). ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks. https://www.iso.org/standard/80585.html. Accessed: 26th August, 2024.

Jacobsson, A. and Davidsson, P. (2015). Towards a model of privacy and security for smart homes. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 727–732. IEEE.

Khosravi-Farmad, M. and Ghaemi-Bafghi, A. (2020). Bayesian decision network-based security risk management framework. *Journal of Network and Systems Management*, 28:1794–1819.

Lee, I. (2020). Internet of things (iot) cybersecurity: Literature review and iot cyber risk management. *Future internet*, 12(9):157.

Luthra, S., Govindan, K., Kannan, D., Mangla, S. K., and Garg, C. P. (2017). An integrated framework for sustainable supplier selection and evaluation in supply chains. *Journal of cleaner production*, 140:1686–1698.

NIST (2024). NIST SP 800-30 - Guide for Conducting Risk Assessments. https://www.nist.gov/privacy-framework/nist-sp-800-30. Accessed: 26th August, 2024.

Palacký University Olomouc (2024). Fuzzy AHP Tool. http://fuzzymcdm.upol.cz/fuzzyahp/. Accessed: 10th August, 2024.

Ramík, J. and Korviny, P. (2010). Inconsistency of pair-wise comparison matrix with fuzzy elements based on geometric mean. *Fuzzy Sets and Systems*, 161(11):1604–1613.

Saaty, T. L. and Vargas, L. G. (1979). Estimating technological coefficients by the analytic hierarchy process. *Socio-Economic Planning Sciences*, 13(6):333–336.

Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., and Sepasgozar, S. M. (2021). Risk management in sustainable smart cities governance: A toe framework. *Technological Forecasting and Social Change*, 167:120743.

Wang, Y., Zhang, R., Zhang, X., and Zhang, Y. (2023). Privacy risk assessment of smart home system based on a stpa–fmea method. *Sensors*, 23(10):4664.

Werner, M. F., Ness, I., and Paupini, C. (2022). Privacy in the smart household: Towards a risk assessment model for domestic iot. In *International Conference on Human-Computer Interaction*, pages 444–454. Springer.