Computer Networks 255 (2024) 110853

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Adaptive learning-based hybrid recommender system for deception in Internet of Thing[☆],[☆☆]

Volviane Saphir Mfogo[a,*], Alain Zemkoho[b], Laurent Njilla[c], Marcellin Nkenlifack[a], Charles Kamhoua[d]

[a] *Department of Mathematics and Computer Science, University of Dschang, P.O. Box 96, Dschang, Cameroon*
[b] *School of Mathematical Sciences, University of Southampton, SO17 1BJ, Southampton, UK*
[c] *Information Assurance Branch, Air Force Research Laboratory, Rome, NY, USA*
[d] *Network Security Branch, US Army Combat Capabilities Development Command Research Laboratory, Adelphi, MD, USA*

ARTICLE INFO

Keywords:
Internet of Things (IoT)
Adaptive learning
Hybrid recommender systems
Deception
Cybersecurity
Vulnerability

ABSTRACT

In the rapidly evolving Internet of Things (IoT) security domain, device vulnerabilities pose significant risks, frequently exploited by cyberattackers. Traditional reactive security measures like patching often fall short against advanced threats. This paper introduces a proactive deception system enhanced by an innovative Adaptive Learning-based Hybrid Recommender System (AL-HRS), utilizing the vulnerability and attack repository for IoT (VARIoT) database. This advanced system identifies existing vulnerabilities and dynamically recommends additional deceptive vulnerabilities based on real-time analysis of attacker behavior and historical exploit data. These recommended vulnerabilities mislead attackers into engaging with controlled environments such as honeypots, effectively neutralizing potential threats. The AL-HRS combines the predictive strengths of content-based filtering (CBF) and collaborative filtering (CF) with an adaptive learning mechanism that adjusts recommendations based on ongoing attacker interactions, ensuring the system's efficacy amidst changing attack patterns. Our approach innovatively combines these methodologies to provide a continuously evolving security strategy, significantly enhancing the deception capability of IoT systems. Initial evaluations demonstrate a potential reduction in device compromise, highlighting the effectiveness and strategic relevance of this adaptive deception framework in IoT cybersecurity.

1. Introduction

The proliferation of the Internet of Things (IoT) has interconnected everything from home appliances to industrial equipment, enriching our daily lives with numerous benefits [1]. However, this connectivity also introduces significant security vulnerabilities, making IoT devices attractive targets for cyber attackers. These vulnerabilities allow unauthorized access, data theft, or operational disruptions, particularly in critical sectors such as healthcare, manufacturing, and transportation [2]. Traditional security measures, such as software updates and patching, are essential yet often reactive. They may fall short in real-time protection due to delays in patch availability or deployment, leaving devices vulnerable [3].

IoT devices frequently share vulnerabilities due to commonalities in the vendor, firmware, or software, which sophisticated attackers exploit. This scenario underscores a critical challenge: the need to effectively obscure real vulnerabilities from attackers. Inspired by recommender systems [4], our approach introduces a proactive deception strategy that presents attackers with alternative, equally plausible vulnerabilities. This not only diverts their focus but also protects real devices by engaging attackers with decoys.

[☆] Distribution A: Approved for Public Release; Distribution is Unlimited.

This research was sponsored by the DEVCOM ARL Army Research Office, USA and was accomplished under Grant Number W911NF-21-1-0326. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

[☆☆] The work of the second author is supported by the EPSRC, UK grant EP/V049038/1 and the Alan Turing Institute, UK under the EPSRC EP/N510129/1.

[*] Corresponding author.
E-mail addresses: smfogo@aimsammi.org (V.S. Mfogo), a.b.zemkoho@soton.ac.uk (A. Zemkoho), laurent.njilla@us.af.mil (L. Njilla), marcellin.nkenlifack@univ-dschang.org (M. Nkenlifack), charles.a.kamhoua.civ@army.mil (C. Kamhoua).

https://doi.org/10.1016/j.comnet.2024.110853
Received 15 May 2024; Received in revised form 30 July 2024; Accepted 7 October 2024
Available online 11 October 2024

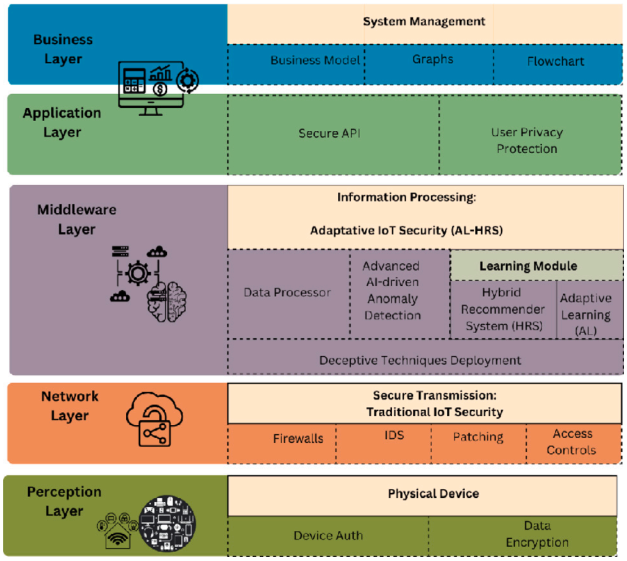


Fig. 1. Overview of IoT architecture and security enhancements introduced by AL-HRS.

We propose a novel hybrid recommender system based on adaptive learning that integrates the strengths of collaborative filtering (CF) and content-based filtering (CBF). This system not only detects but also predicts potential vulnerabilities based on both past exploit behaviors and intrinsic vulnerability characteristics. The hybrid model dynamically adjusts its recommendations by learning from ongoing interactions, which significantly enhances its predictive accuracy and adaptability in a changing threat landscape.

This paper introduces a deception framework that leverages an advanced hybrid recommender system based on adaptive learning to enhance IoT security. By combining CF's pattern recognition capabilities with CBF's detailed attribute analysis, the proposed system efficiently identifies and suggests deceptive vulnerabilities. These decoys are designed to mimic real vulnerabilities in credibility, complexity, and appeal, thus protecting network integrity while collecting valuable intelligence on attacker strategies and tools.

Fig. 1 presents a detailed overview of the conventional IoT architecture across its multiple layers, from the Perception Layer up through the Business Layer. This illustration clarifies the traditional security processes employed at each layer and showcases the novel enhancements introduced by our Adaptive Learning-based Hybrid Recommender System (AL-HRS), particularly within the Middleware Layer. The integration of AL-HRS significantly augments traditional security measures, offering advanced anomaly detection and adaptive defensive strategies crucial for tackling the sophisticated threats faced in modern IoT environments. This architecture addresses the current research landscape, highlighting both our adherence to and evolution beyond traditional security paradigms.

To the best of our knowledge, this is the first work to implement an adaptive learning-based hybrid recommender system specifically designed to enhance IoT security by integrating deceptive vulnerabilities into a proactive defense mechanism. The main contribution of this work is the development of the AL-HRS for IoT security, which significantly enhances network security by deploying a deceptive layer that actively misleads attackers. An empirical evaluation demonstrates the effectiveness of the system in increasing the engagement time with the decoys and reducing the success rate of attacks, thus leading to a reduction in device compromise. These results highlight the effectiveness of the proposed approach in creating a more secure IoT environment.

Following this introduction, Section 2 discusses related work in IoT security and deception techniques. Section 3 details our methodology, integrating the hybrid recommender system with the IoT security framework. Section 4 evaluates the performance of the system and discusses its practical implications. Finally, Section 5 concludes the paper and outlines future research directions in this evolving domain.

2. Background and related work

2.1. Background

2.1.1. IoT security measures

The landscape of IoT security has evolved significantly, reflecting the rapid advancement and increasing ubiquity of IoT devices in various sectors [5,6]. Initially, the focus on IoT security was on basic measures such as network protection. However, as the applications of this technology expanded into more critical areas, the demand for more sophisticated security strategies became unavoidable. These advanced measures aim to address the unique vulnerabilities introduced by the extensive interconnectivity and diversity of IoT devices, underscoring the complexity of securing vast networks against a wide array of ever-evolving cyber threats [7].

The common vulnerability scoring system (CVSS) plays a pivotal role in this context by providing a standardized framework to assess and prioritize IoT vulnerabilities based on their severity and potential impact [8]. This scoring system is crucial for the development of targeted security responses, ensuring that priority is given to the most critical vulnerabilities first. In recent developments, there has been an exploration into the strategic use of fabricated vulnerabilities as a method to deceive and redirect attackers [9–12]. These studies illuminate the complexities of using fake vulnerabilities effectively—while they can serve as potent tools for misdirection, they also pose significant challenges. These include maintaining their believability to ensure that they are not easily distinguishable from real vulnerabilities and managing the resource drain on security teams tasked with maintaining them to ensure they remain effective and do not inadvertently compromise the system [13].

In addition, modern cybersecurity strategies increasingly incorporate advanced deception techniques. What started with basic honeypots has evolved into sophisticated deception architectures that employ a variety of decoys and artificially generated data to actively engage and mislead attackers [14,15]. This proactive approach does more than just detect intrusions; it interacts with attackers, diverting them from real targets, and gathering crucial intelligence about their tactics and strategies. This shift towards an active defense mechanism enhances the capacity to develop stronger and more effective security measures.

2.1.2. Recommender system

Simultaneously, the role of recommender systems in cybersecurity has become increasingly prominent. Traditionally used in commercial settings to enhance user experiences by personalizing content recommendations, these systems are now being adapted for cybersecurity applications. They analyze user data to predict and present the most relevant information, significantly helping to quickly identify threats and vulnerabilities [16,17]. The integration of recommender systems into cybersecurity represents a major shift towards managing the overwhelming volumes of data inherent in modern security operations, enhancing the efficiency of detection and response strategies.

A particularly innovative development in the area of recommender systems is the emergence of hybrid recommender systems, which merge the data-driven insights of CF with the attribute-specific analysis of CBF [18]. These hybrid systems adaptively leverage both historical interaction data and specific item attributes to provide precise and contextually relevant item recommendations.

2.2. Related work

This section reviews the relevant literature in three primary domains that intersect in our study: IoT security, deception techniques, and the application of recommender systems in cybersecurity. These domains provide the foundational knowledge necessary to understand the innovative approach of our work.

2.2.1. IoT security

The security of IoT devices is a critical area of concern due to their proliferation and integration into key sectors such as healthcare, manufacturing, and transportation [5,6]. Chen et al. [19] highlight the dynamic challenges in securing diverse IoT devices against evolving cyber threats, emphasizing the necessity for adaptive security protocols. Similarly, Siwakoti et al. [20] discuss vulnerabilities that arise from the interconnectivity of IoT devices, such as cascading failures, underscoring the need for robust network security strategies. Research in this domain underscores the complexity of managing security in an expansive network of diverse devices, each with its unique vulnerabilities [7, 21,22].

2.2.2. Deception techniques in cybersecurity

Deception techniques have become a cornerstone of modern cybersecurity strategies, evolving from simple honeypots to complex systems that employ a variety of decoys and simulated vulnerabilities to mislead attackers [14,23]. These advanced strategies are designed not only to detect unauthorized access but also to engage attackers actively, thereby diverting them from real targets and gathering intelligence about their tactics and strategies. Studies like those by Pour et al. [15] highlight the sophistication of these systems, which can dynamically react to attacker behaviors, thus offering deeper insights into potential security breaches.

However, despite their effectiveness, many current deception frameworks, such as adaptive intelligent interaction honeypots, depend heavily on collecting extensive data from interactions between attackers and IoT devices [24,25]. These systems often require detailed request/response data to learn and adapt, which limits their applicability in environments where such data is scarce or sensitive [23]. This dependency reveals a gap in the current landscape of deception technologies—there is a need for methods that can operate effectively without relying on extensive prior data, learning dynamically from limited interactions.

To highlight the significance and innovation of our study, we include a comparison table contrasting key features and outcomes of existing IoT security solutions with our proposed system. Table 1 elucidates the advanced capabilities of our approach, particularly in terms of adaptability, accuracy, and deception strategies level.

The CVSS plays a pivotal role in the assessment and prioritization of security threats in IoT environments. By providing a standardized framework to evaluate the severity of vulnerabilities, CVSS helps organizations allocate their defensive resources more effectively [8]. In our research, we utilize CVSS scores to enhance the realism of the deceptive vulnerabilities introduced into IoT systems. By aligning our decoys with vulnerabilities that reflect actual CVSS scores, our approach not only increases the credibility of the decoys but also ensures that they are perceived as genuine threats by attackers, thus enhancing the overall effectiveness of the deception strategy. This integration of CVSS into our deception framework ensures that our security measures are both proactive and responsive, capable of adapting to the evolving landscape of cyber threats while effectively misleading potential attackers.

2.2.3. Recommender systems in cybersecurity

Recommender systems, traditionally used in commercial settings to enhance user experience, are now being adapted for cybersecurity applications. These systems play a crucial role in efficiently filtering and prioritizing security-related information, which enhances cyberattack detection and prevention efforts. Pawlicka et al. [17] explored how recommender systems can manage information overload and improve decision-making in security operations centers. Meanwhile, Huff et al. [26] proposed a recommender system designed to automatically identify a minimal candidate set of common software product enumerators for software names, which helps improve vulnerability identification and alert accuracy. However, existing studies lack exploration of using recommender systems to propose a deceptive system.

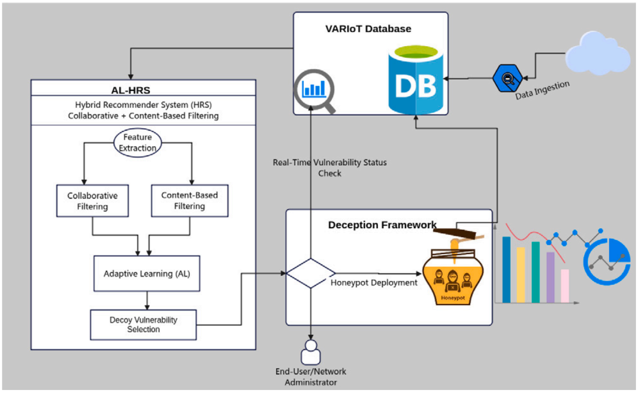


Fig. 2. Architecture of the Adaptive learning-based Hybrid Recommender System (AL-HRS) for IoT security. The system is structured around three main components: the AL-HRS, the VARIoT database, and the deception framework. The AL-HRS utilizes both collaborative and content-based filtering to process IoT device data and vulnerabilities from the VARIoT database. This database continuously updates and ingests new data to ensure real-time vulnerability status checks. Based on this data, the AL-HRS performs feature extraction and utilizes adaptive learning algorithms to refine the selection of decoy vulnerabilities, which are then deployed via the deception framework. The deception framework creates honeypot environments that mimic real IoT device vulnerabilities, fooling attackers and protecting real network infrastructure.

2.2.4. Hybrid recommender systems and IoT security

CF and CBF, hybrid recommender systems address the limitations found in each method separately. CF is effective in identifying patterns based on user interaction data but struggles with the cold start problem. CBF offers precise recommendations based on item attributes but may overlook complex user preferences [27,28]. Widayanti et al. [18] highlight how hybrid systems that amalgamate these methodologies can improve the precision and relevance of security recommendations in IoT contexts. Our work extends this approach by integrating adaptive learning mechanisms, enhancing the system's ability to respond to evolving threats in real time.

3. Recommended deceptive defense

This section delves into the construction of a deceptive defense strategy that leverages the capabilities of an adaptive learning-based hybrid recommender system (AL-HRS) for IoT security. The strategy is designed to mislead attackers by dynamically presenting them with deceptive vulnerabilities, thereby protecting real devices.

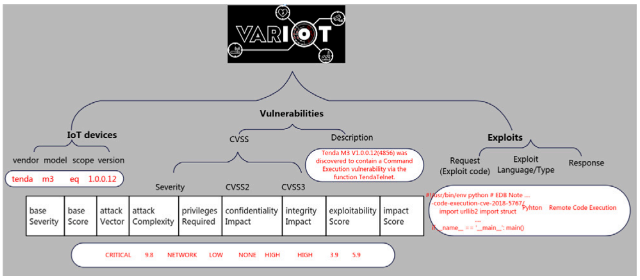
3.1. Overview

The architecture of our system is depicted in Fig. 2. It is crafted to integrate perfectly with existing IoT networks and consists of three main components: the VARIoT database, the AL-HRS and the deception framework. This setup illustrates how these components interact to enhance IoT security through proactive deception.

- **VARIoT database:** This database serves as the backbone of our system, containing extensive data on IoT vulnerabilities and exploits [29]. It is continuously updated to reflect the latest security findings and trends in IoT vulnerabilities, sourced from multiple databases and security publications such as the common vulnerabilities and exposures (CVE) and national vulnerability database (NVD) [30]. This real-time update mechanism ensures that the recommendations of our system are based on the most current data available.
- **AL-HRS:** At the heart of our methodology lies AL-HRS, which analyzes vulnerability data from the VARIoT database alongside real-time feedback on attacker behaviors and interactions with decoy systems. This system employs a sophisticated blend of

Table 1
Comparison of key features and outcomes of existing IoT security solutions.

Reference	Key findings	Adaptability	Accuracy	Deception strategies	Limitations
Chen et al. (2022) [19]	Highlights dynamic challenges in securing diverse IoT devices against evolving cyber threats, emphasizing adaptive security protocols.	High	92% accuracy in threat detection.	Focuses on threat detection rather than deception.	High complexity in managing security for diverse devices.
Siwakoti et al. (2023) [20]	Discusses vulnerabilities from the interconnectivity of IoT devices, such as cascading failures, underscoring the need for robust network security strategies.	Moderate	Identified and mitigated 85% of cascading failures.	Primarily focused on network security, not deception.	Focuses mainly on network security without addressing individual device security.
Pour et al. (2022) [15]	Demonstrates a proactive deception technique that can dynamically react to attacker behaviors.	High	Achieved 60% higher engagement with attackers compared to static honeypots.	Focuses on proactive engagement.	Requires detailed request/response data, which may not be available in all environments.
Mfogo et al. (2023) [24]	Proposes an adaptive honeypot that interacts intelligently with attackers to gather data and improve security measures.	High	Increased attacker engagement by 40%.	Provides valuable data for enhancing security protocols.	Complexity in implementation and maintenance.
Huff et al. (2021) [26]	Proposes a system designed to identify common software product enumerators for software names, improving vulnerability identification.	Low	Improved vulnerability identification accuracy by 25%.	Does not focus on deception strategies.	Limited applicability beyond identifying software product vulnerabilities.
Widayanti et al. (2023) [18]	Highlights how hybrid systems can improve the precision and relevance of security recommendations in IoT contexts.	Moderate	Increased recommendation precision by 15%.	Focuses on recommendation accuracy rather than deception.	Focuses on general applications without specific emphasis on cybersecurity.
Our approach	**Integrates adaptive learning-based hybrid recommender system for proactive IoT security and deception.**	**High**	**92% accuracy in recommending deceptive vulnerabilities.**	**Dynamically adjusts and deploys effective decoys.**	**Ongoing need for system updates and monitoring.**



Tenda M3 V1.0.0.12(4856) was discovered to contain a Command Execution vulnerability via the function TendaTelnet.

```
#!/usr/bin/env python # EDB Note ....
-code-execution-cve-2018-5767/
import urllib2 import struct
....
if __name__ == '__main__': main()
```

Fig. 3. VARIoT database entries.

CF and CBF, enhanced by adaptive learning algorithms. These algorithms adjust the recommendation logic based on the effectiveness of past decoys, optimizing future recommendations to ensure they remain compelling to attackers without being predictable.

- **Deception framework:** The recommendations generated by the AL-HRS are operationalized through the deception framework. This component deploys controlled environments or honeypots that simulate the vulnerabilities suggested by the AL-HRS. These environments are meticulously crafted to mimic actual IoT device vulnerabilities, complete with simulated responses to attack attempts. This not only diverts the attacker from real targets but also allows for the collection of intelligence on attack methods, which feeds back into the AL-HRS to refine further recommendations.

3.2. Detailed VARIoT database structure

The database we used in this work is structured into two main sections: vulnerabilities and exploits each providing valuable data obtained from curated primary sources and Internet search engines such as the CVE and NVD. Its relevance lies in the accurate and up-to-date profiling of IoT device vulnerabilities, which is critical for our system's ability to recommend plausible deceptive vulnerabilities alongside actual ones. The dataset's depth and breadth provide a robust platform for understanding and simulating real-world IoT security scenarios. As shown in Fig. 3, each database entry is composed of the IoT device characteristics (e.g., manufacturer/vendor, device type, operating system, firmware version, and network settings), the vulnerability characteristics (e.g., severity, description, and impact) and the exploit (e.g., the exploit request/response)

3.2.1. IoT vulnerabilities

VARIoT is a dynamic repository that provides timely updates on IoT device vulnerabilities. It uses the power of machine learning and natural language processing to merge information from diverse sources, yielding detailed vulnerability descriptions and classifications [29]. As depicted in Fig. 3, the database meticulously records essential details for each affected device, including vendor, model, scope, and version. In addition, it evaluates the vulnerabilities based on the severity and type defined by the CVSS, as well as the current status of each vulnerability, ensuring that our recommender system can make precise and contextually relevant suggestions.

3.2.2. IoT exploits

This section of the VARIoT database catalogs publicly available exploits targeting IoT devices, enriched by an ontology detailing their attributes and potential impacts. Currently, for the development of the repository, this section aims to mirror the detailed structuring found in Section 3.2.1. It plays a crucial role in our deception strategy by providing real-world data on exploit techniques that, when analyzed, act as feedback from attackers. This feedback is instrumental in understanding which vulnerabilities are most frequently exploited, thereby enabling our system to recommend the most effective deceptive vulnerabilities for specific IoT devices.

To address the complexity of translating diverse exploits from the VARIoT database into actionable decoys, our system employs a multi-layered translation mechanism. This mechanism first categorizes exploits based on their attack vectors and impact severity, utilizing a rule-based classification system. Subsequently, it uses a set of containerized environments, each tailored to simulate specific exploit behaviors. These environments are dynamically configured with sandboxing techniques to ensure they accurately reflect the operational characteristics of the exploits while isolating them from the main network. This improves the realism of the decoys but also preserves system integrity and prevents leakage between the deceptive and real environments.

3.3. Adaptive learning-based hybrid recommender system (AL-HRS)

The AL-HRS is designed to dynamically recommend deceptive vulnerabilities to IoT devices, effectively engaging potential cyber attackers. This system integrates CF and CBF enhanced with an adaptive learning mechanism, evolving through real-time feedback on attacker behaviors and deception effectiveness. The AL-HRS leverages a mix of static and dynamic features to form comprehensive vulnerability and device profiles.

- **Static features** (CBF):
  - *Vulnerability Attributes*: Type, severity, related software/hardware;
  - *Device Attributes*: Manufacturer, device type, firmware version.
- **Dynamic features** (CF):
  - *Exploit Patterns*: Historical exploit attempts, frequency, and recency.

3.3.1. Collaborative and content-based filtering mechanisms

CF and CBF are two principal methodologies utilized in our AL-HRS to enhance the security framework for IoT devices by recommending plausible deceptive vulnerabilities.

CF operates by analyzing the interaction data of various attackers to predict potential vulnerabilities that similar attackers might exploit. In the IoT security context:

- The interaction data includes exploit attempts on IoT devices, which provides insights into the vulnerabilities preferred by different types of attackers;
- To identify patterns that indicate how attackers exploit similar devices or vulnerabilities, thus predicting which vulnerabilities might be next targeted.

CBF leverages the attributes of the items themselves (vulnerabilities and devices) to make recommendations, focusing on properties that have previously attracted attacks. For IoT security, this involves:

- Attributes of vulnerabilities such as their severity, exploitability, and impact scores (from CVSS), alongside device-specific details like firmware version, type, and manufacturer.
- To recommend vulnerabilities based on their similarity to those previously exploited, considering specific attributes that may attract attackers.

Hybrid recommendation score: The integration of CF and CBF is achieved using a weighted sum approach, dynamically adjusted by an adaptive learning mechanism. The recommendation score for a vulnerability v_j on a device d_i is calculated as follows:

$$\begin{aligned}\text{Score}(v_j, d_i) = {} & \theta_{CF} \cdot \text{CF\_Score}(v_j, d_i) \\ & + \theta_{CBF} \cdot \text{CBF\_Score}(v_j, d_i),\end{aligned} \tag{1}$$

where:

- θ_{CF} and θ_{CBF} are the adaptive weights assigned to the outputs from CF and CBF, respectively;
- $\text{CF\_Score}(v_j, d_i)$ quantifies the relevance of a vulnerability based on interaction patterns of attackers with similar profiles;
- $\text{CBF\_Score}(v_j, d_i)$ reflects the relevance based on the intrinsic attributes of the vulnerabilities and device profiles.

This hybrid approach allows AL-HRS to leverage the comprehensive analytical strengths of both CF and CBF, enhancing the system's capability to devise effective deceptive strategies in IoT security. The adaptive learning mechanism, specifically a Markov Decision Process (MDP), continuously fine-tunes θ_{CF} and θ_{CBF} based on real-time feedback to maximize the effectiveness of the deception.

Markov decision process (MDP): An MDP is a mathematical framework used for modeling decision-making in situations where outcomes are partly random and partly under the control of a decision-maker [31]. MDPs are used extensively in reinforcement learning (RL) to determine optimal policies—sequences of decisions that achieve the best-expected outcome [32]. At each step within an MDP, the system's state may change in response to the actions taken, governed by transition probabilities. The primary objective of an MDP is to identify a policy that maximizes the expected reward over time, considering the uncertainties in state transitions and rewards. MDPs provide a structured way to make a series of decisions by considering both the immediate and future states. This is essential in environments where each decision impacts future opportunities and risks. These are used to model the likelihood of moving from one state to another, based on the action selected. The transition model defines the dynamics of the environment. In this context, RL is used to iteratively improve the decision-making policy. An RL agent learns from interactions with the environment by receiving rewards or penalties and adjusting its actions based on past experiences to maximize cumulative rewards.

This MDP framework is crucial for adaptive systems like the proposed AL-HRS, which dynamically adjusts its strategies to optimize the effectiveness of deception in IoT security by learning from the outcomes of past actions and their consequent rewards. Our approach strategically links real IoT devices with their deceptive counterparts to enhance the believability of the network's defensive measures. By mirroring actual network traffic and device behaviors in the decoys, we significantly increase the difficulty for attackers to distinguish between real and fabricated vulnerabilities. This linkage is crucial for maintaining a high engagement rate with the decoys, thereby effectively diverting potential threats. Additionally, this method allows for the continuous refinement of our deception strategies based on observed attacker interactions with both real and fake assets, ensuring a robust adaptive defense system.

3.3.2. Adaptive learning for weight optimization

The AL-HRS utilizes an RL framework specifically tailored to dynamically adjust the weights θ_{CF} and θ_{CBF}. These weights critically determine the balance between CF and CBF outputs in our hybrid recommendation model, thereby optimizing the system's deception effectiveness against potential cyber attackers.

Problem formulation. The AL-HRS system interacts with an IoT ecosystem through an MDP, modeling its environment where the agents (recommendation system) and environment (attackers) engage. The aim is to learn a strategy that maximizes the effectiveness of the deception through adaptive actions:

- **States** (s): these are defined by the current security status of the IoT environment, which includes detected attack patterns and known vulnerabilities;
- **Actions** (a): these involve selecting which vulnerabilities to present as decoys, intended to misdirect attackers effectively;
- **Rewards** (r): they are assigned based on the deception's success, measured by how effectively attackers are misled by the decoys;

- **Transition probabilities** (T): Transition probabilities dictate the likelihood of moving from one state to another following an action, influenced by the attacker's response to the deception strategies implemented.

Reinforcement learning algorithm. We apply Q-learning, an RL algorithm, which optimizes the weights θ_{CF} and θ_{CBF}, integrating them to refine the hybrid recommendation strategy:

$$Q(s_t, a_t) = r(s_t, a_t) + \gamma \max_a Q(s_{t+1}, a), \tag{2}$$

where γ is the discount factor, emphasizing the importance of immediate rewards over distant future rewards.

Reward function. The reward function is designed to reinforce actions that effectively deceive attackers:

- **Positive rewards** are granted for actions leading to successful engagements with decoys;
- **Negative rewards** are applied to actions that fail to engage or lead to the detection of decoys by attackers.

Update rule. The update rule adjusts θ_{CF} and θ_{CBF} based on learned Q-values to continuously improve the decision-making process:

$$\begin{aligned} Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \, [r(s_t, a_t) \\ + \gamma \max_a Q(s_{t+1}, a) - Q(s_t, a_t) \,], \end{aligned} \tag{3}$$

where α represents the learning rate, facilitating the rate at which new information is incorporated.

Exploration vs. Exploitation. An ϵ-greedy approach manages the trade-off between exploring new strategies and exploiting known effective strategies to optimize the learning trajectory and avoid local minima.

Online Q-learning algorithm. This system is designed for real-time adaptability to emerging threats and shifts in attacker behaviors, continuously refining and updating its strategies based on active interactions and feedback within the IoT environment. The algorithm 1 systematically describes how the AL-HRS operates. This algorithm originally inspired by the principles of reinforced learning, our enhancements to this algorithm include the integration of a new decision-making layer that leverages a CF and CBF. These enhancements allow for more dynamic response patterns based on real-time IoT data analysis. Additionally, Algorithm 2, Online Q-learning for AL-HRS, is an original creation designed to optimize the real-time adaptation of the recommender system's weighting parameters. This algorithm employs an ϵ-greedy policy combined with Q-learning, a method not previously applied within the context of IoT security in this manner. This unique approach allows the system to dynamically adjust its strategy based on ongoing attacker interactions, significantly enhancing the adaptability of our security measures. The algorithm's novelty lies in its ability to continuously refine the decision-making process, ensuring high effectiveness even in the face of complex and evolving threats.

This focused reinforcement learning approach ensures that AL-HRS remains both responsive and proactive, adeptly adjusting θ_{CF} and θ_{CBF} to enhance the deception capabilities against evolving cyber threats, maintaining robust security measures within the IoT domain.

Algorithm 1 AL-HRS: Adaptive Learning-based Hybrid Recommender System

```
Initialization:
Initialize $\theta_{CF}$, $\theta_{CBF}$ for CF and CBF.
Load or initialize Q-table from previous sessions, if available
Configure parameters: learning rate $\alpha$, discount factor $\gamma$, exploration rate $\epsilon$
while IoT system is active do
    Collect current IoT device profiles, vulnerability and historical exploit data
    Construct feature vector $\mathbf{x}_i$ for current device $d_i$ from $\mathbf{p}_i$ (profiles), $\mathbf{v}_i$ (vulnerabilities), $\mathbf{e}_i$ (exploit history).
    Calculate CF and CBF scores for potential vulnerabilities
    Obtain recommendation scores using current weights:
        $\text{Score}(v_j, d_i) = \theta_{CF} \cdot \text{CF\_Score}(v_j, d_i) + \theta_{CBF} \cdot \text{CBF\_Score}(v_j, d_i),$    (4)
    Call Algorithm 2 to adjust $\theta_{CF}$, $\theta_{CBF}$ based on reward signals
    Deploy recommended vulnerabilities based on updated recommendation scores
    Monitor attacker interactions and collect feedback.
    Validate and refine recommendations through simulations.
end while
```

Algorithm 2 Online Q-learning for AL-HRS

```
while receiving feedback from the IoT environment do
    Observe current state $s_t$ (current security context and attacker interactions)
    Select action $a_t$ (choose weights to apply) using $\epsilon$-greedy policy:
    if random() < $\epsilon$ then
        Choose a random set of weights
    else
        Choose weights that maximize current Q-values:
            $a_t = \arg\max_a Q(s_t, a)$
    end if
    Apply weights, observe reward $r_t$ and new state $s_{t+1}$
    Update Q-values:
        $Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \left[ r_t + \gamma \max_a Q(s_{t+1}, a) - Q(s_t, a_t) \right]$
    Optionally adjust $\epsilon$ to reduce exploration over time
end while
```

3.4. Deception framework

Our deception framework operates by strategically integrating both real and recommended vulnerabilities into the security profiles of IoT devices, as recommended by the AL-HRS. This framework not only masks real vulnerabilities but also engages potential attackers with meticulously crafted decoys, directing them towards controlled environments designed to simulate actual device vulnerabilities. Therefore, before deploying any deceptive measures, it is critical to ensure that the system can accurately distinguish between legitimate users and potential attackers. Drawing from established methodologies in behavioral analytics and anomaly detection [33,34], our system implements advanced monitoring techniques to analyze access patterns and interaction behaviors. This initial filtering ensures that normal user activities are not disrupted by the deception tactics aimed at attackers, preserving the seamless operation of IoT devices while enhancing security.

Integration of vulnerabilities. Upon identifying a real vulnerability within a device, the system first verifies its current status against the VARIoT database. If the vulnerability has been resolved, the system either automatically applies a security patch or alerts network administrators to take immediate action. This proactive posture ensures that vulnerabilities are addressed promptly, safeguarding the network against potential exploits.

Deployment of decoys. Simultaneously, the system enhances the device's security profile by integrating recommended fake vulnerabilities. These are presented alongside real vulnerabilities to create a nuanced security facade that misleads attackers. Each deceptive vulnerability is paired with a corresponding honeypot, which mimics the characteristics of the supposed vulnerability. For instance, if a vulnerability related to an open Transmission Control Protocol (TCP) port is suggested, a honeypot simulating an open port is deployed. This not only diverts the attacker from actual network assets but also allows for the monitoring and analysis of attack methods in a risk-free environment.

Honeypot operations. When attackers target these fake vulnerabilities, they are redirected to the honeypots. These honeypots [24] are sophisticated enough to engage attackers convincingly, thereby protecting the real systems and collecting critical data on attack patterns and techniques. This intelligence is crucial for continually refining the deception strategies and updating the AL-HRS recommendations.

Feedback loop. All interactions within these honeypots are logged and analyzed, with significant exploits stored back into the VARIoT database. This continuously enriches the data available for future recommendations, ensuring that the deception framework remains dynamic and responsive to evolving cybersecurity challenges. This cyclical process not only mitigates immediate threats but also enhances the long-term resilience of IoT environments against cyberattacks.

3.5. Use case and implementation

In this part, we present a use case that illustrates how our system can enhance IoT security by combining accurate vulnerability assessment with strategic deception, turning potential security weaknesses into opportunities for defense and intelligence gathering.

3.5.1. System integration and workflow: Threat model

The integration of our components into IoT networks is designed to be seamless and minimally intrusive, yet robust against specific cybersecurity threats. Our threat model assumes a landscape where attackers continually scan IoT devices to exploit known vulnerabilities. In response, our system employs the VARIoT database, which is continuously updated with the latest vulnerability data. This data is crucial for the AL-HRS to operate effectively. AL-HRS leverages feedback from previous engagements with attackers, including data on which vulnerabilities (decoys) were exploited and the tactics used. This feedback refines the system's predictive models, employing adaptive learning techniques to anticipate and simulate new, plausible deceptive vulnerabilities.

These recommended vulnerabilities are strategically incorporated into our deception framework. They create detailed, fictitious, yet realistic profiles of device vulnerabilities. When attackers scan the network, they encounter these decoy profiles, leading them into honeypots that simulate the fake vulnerabilities. This deceptive strategy neutralizes the threats by diverting attackers from real targets and engaging them in a controlled environment. This not only mitigates immediate risks but also collects valuable intelligence on attack patterns and tactics, thereby enriching our understanding of the threat landscape and continuously improving the system's defensive capabilities and accuracy.

3.5.2. Example scenario: Securing an IP camera

Consider an IP camera connected to an IoT network, commonly targeted by cyberattackers due to its access to sensitive visual data. Initially, our system integrates with the network and identifies any known vulnerabilities in the specific IP camera model. For instance, it might discover a vulnerability related to *unsecured data transmissions*.

Vulnerability analysis and recommendation. Upon identifying real vulnerabilities, the recommender system analyzes their characteristics—such as nature, severity, CVSS score, and device type. It then leverages this analysis to select additional, plausible vulnerabilities based on AL-HRS that could exist in similar devices but are not yet identified or exploited, such as *open TCP ports or firmware exploits*. This creates a comprehensive profile of the IP camera that integrates real and recommended (deceptive) vulnerabilities.

Deception strategy implementation. The comprehensive vulnerability profile is then embedded in a virtual representation of the IP camera within our deception framework. This virtual profile acts as a digital façade, showcasing real and deceptive vulnerabilities. It is presented to the network through techniques such as port mirroring or network traffic redirection, ensuring attackers encounter this façade rather than the actual device. Network responses are simulated to reflect the vulnerabilities in the façade, such as responding to queries that target these fake vulnerabilities.

Engagement with attackers. If a user detected as an attacker targets the recommended vulnerabilities, such as attempting to exploit the *open TCP port*, they are seamlessly redirected to a honeypot. This honeypot is meticulously configured to emulate an IP camera with the specified vulnerabilities, thus creating the illusion of a successful breach. Interaction within this controlled environment is monitored in detail, recording the attacker's tactics, tools used, and the nature of the exploitation attempt. This provides valuable information on current attack methodologies and helps identify specific threat actors.

Simultaneously, the actual IP camera is secured by addressing its real vulnerabilities through recommended patches or updates, based on the system's analysis. The honeypot not only diverts attackers but also serves as a tool for continuous learning and system refinement, allowing it to adapt to evolving attack patterns. This ensures the ongoing security of the network while engaging potential attackers harmlessly, thereby safeguarding the network and enhancing our understanding of cyber threats.

4. Evaluation

In this section, we first describe the evaluation setup, metrics, and general performance of AL-HRS. Then, we conduct a comparative performance analysis of AL-HRS and the existing deception approach.

4.1. Evaluation criteria setup

To ensure a comprehensive assessment of the AL-HRS, our evaluation strategy is meticulously crafted to reflect real-world IoT environments, specifically focusing on smart home ecosystems. This rigorous approach is crucial for demonstrating the system's effectiveness, scalability, and adaptability under realistic conditions.

4.2. Simulation test environment

Our simulation test environment is meticulously designed on a virtualized platform hosted on the Google Cloud Platform (GCP). This setup emulates a network of IoT devices commonly found in smart homes, including smart thermostats, refrigerators, cameras, and other consumer electronics, as detailed in Table 2.

Each device is configured with common vulnerabilities and realistic operational profiles to closely simulate authentic behaviors and interactions observed in IoT environments. The device vulnerabilities are sourced from the CVE and NVD, ensuring that all vulnerabilities used are publicly disclosed and affect real-world devices.

We presume each device features at least one exploitable vulnerability, potentially granting root privileges to an attacker. This setup allows for the exploration of various security scenarios where additional vulnerabilities could be integrated, depending on the complexity and desired depth of the simulation. The vulnerability information for each device is meticulously represented by the VARIoT database to provide a realistic and challenging environment for testing the effectiveness of the AL-HRS.

4.2.1. Simulated attack scenarios

The robustness of AL-HRS is tested using a comprehensive suite of simulated attack scenarios. These include not only common threats like

Table 2
Smart home devices and their vulnerabilities.

Device type	CVE ID	Affected vendor/Component	CVSS exploitability	Compromise rate (per day)
Smart thermostat	CVE-2022-2185	Nest Thermostat	7.8	0.006
Smart light	CVE-2023-0012	Philips Hue	7.5	0.006
Smart fridge	CVE-2022-3036	Samsung Family Hub	9.0	0.012
Home security camera	CVE-2023-0048	Arlo Pro	10.0	0.042
Smart TV	CVE-2022-2097	LG Smart TV	8.6	0.012
Home assistant hub	CVE-2023-0110	Amazon Echo	6.5	0.004
NAS server	CVE-2023-0222	Synology DS220j	10.0	0.042

reconnaissance, SQL injections and brute force attacks but also more sophisticated challenges such as advanced persistent threats (APTs), zero-day exploits, and multi-vector attack campaigns. These scenarios are executed using a mixture of automated scripts and controlled manual penetration testing, designed to simulate widespread and targeted cyber threats, providing a detailed examination of the defensive capabilities of the system.

4.2.2. Real-time adaptation and response testing

The dynamic adaptability of AL-HRS is evaluated through continuous attack simulations, where the system's responses are monitored in real-time. This includes adjusting the deceptive strategies on the fly, effectively recalibrating and redirecting attacks towards honeypots, and analyzing the system's ability to learn from ongoing interactions to enhance its defensive measures.

These simulations are not merely theoretical but are tailored to expose AL-HRS to a variety of plausible threat scenarios a smart home IoT device might face, ensuring the system is practically effective in operational contexts. This evaluation setup ensures that AL-HRS is tested in conditions that mimic real-world challenges, demonstrating its ability to protect IoT environments effectively.

4.3. Evaluation metrics

Our evaluation used several key metrics to measure the performance and impact of AL-HRS.

- **Recommender system accuracy:** Precision, recall, and F1 scores were calculated to assess how accurately AL-HRS identified and suggested deceptive vulnerabilities, providing a quantitative measure of its effectiveness in misleading attackers.
- **Effectiveness of deception strategy:** We quantified the success of the system in engaging attackers with decoys and diverting them from real targets, evaluating the trustworthiness and practical deception capabilities of AL-HRS.
- **Comparative analysis of recommender systems:** AL-HRS was compared against traditional and established recommender systems used in cybersecurity, highlighting its advancements and improvements in handling adaptive threats and real-world applicability.

Additionally, the system's operational effectiveness in deploying deceptive strategies was measured against traditional deception techniques, such as simple honeypots or basic decoy networks.

- **Attacker engagement time:** This metric tracked the duration for which attackers engaged with the honeypots, indicative of the decoys' believability and engagement capacity.
- **Detection rate:** We measured how effectively the system detected and responded to exploitation attempts, a key indicator of its proactive defensive capabilities.
- **Number of attacker actions:** This count helped understand the complexity and persistence of the attack patterns, assessing the efficacy of the decoys in maintaining attacker interest.
- **System scalability:** The ability of AL-HRS to scale up and manage an increasing number of devices without performance degradation was evaluated, critical for its application in extensive IoT networks.

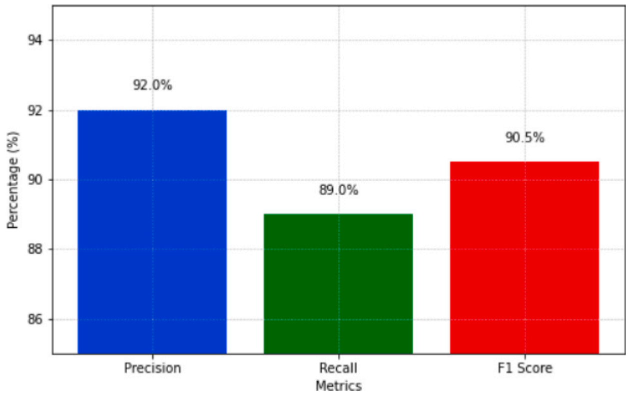


Fig. 4. Average Precision, Recall, and F1 score of AL-HRS across different testing environments, illustrating the system's capability in accurately identifying and recommending deceptive vulnerabilities.

Table 3
Comparison of accuracy metrics across different systems.

System	Precision	Recall	F1 score
AL-HRS	92%	89%	90.5%
Hybrid CF+CBF	85%	82%	83.5%
CF only	80%	78%	79.0%
CBF only	78%	75%	76.5%

These comprehensive metrics collectively underscored AL-HRS's ability to effectively respond to and mitigate evolving cyber threats, reinforcing the security of IoT environments.

4.4. Evaluation results

This section presents the results derived from the comprehensive testing of the AL-HRS. The evaluation was designed to assess the system under various conditions and setups, providing a well-rounded analysis of its effectiveness.

4.4.1. Accuracy metrics

As illustrated in Fig. 4, AL-HRS achieved an average precision of 92%, reflecting the system's proficiency in identifying suitable deceptive vulnerabilities for various attack scenarios. The recall rate was 89%, indicating the system's ability to fully identify exploitable vulnerabilities in simulated IoT devices. The overall F1 score reached 90.5%, demonstrating the balanced precision of AL-HRS in making deception-based recommendations. AL-HRS demonstrated superior performance in precision, recall, and F1 score compared to other systems, as depicted in Fig. 4 and Table 3.

Table 4 lists some of the vulnerabilities recommended by AL-HRS for each device type in the simulated smart home environment. Each entry in this table specifies the type of vulnerability, the expected CVSS exploitability score, and the effectiveness of the decoy in engaging potential attackers. These recommended vulnerabilities serve as decoys intended to mislead attackers and analyze their interaction patterns.

Table 4
Recommended vulnerabilities for smart home devices.

Device type	CVE ID	Recommended vulnerability	CVSS exploitability	Effectiveness
Smart thermostat	CVE-2023-5002	Buffer overflow in communication protocol	8.5	High
Smart light	CVE-2023-5003	Firmware reversion attack	7.1	Medium
Smart fridge	CVE-2023-5004	Cross-site scripting in web interface	6.9	Medium
Home security camera	CVE-2023-5005	Remote code execution via API	9.8	High
Smart TV	CVE-2023-5006	Denial of service through malformed inputs	7.5	Medium
Home assistant hub	CVE-2023-5007	Eavesdropping vulnerability in voice commands	8.2	High
NAS server	CVE-2023-5008	SQL injection in device management interface	9.0	High

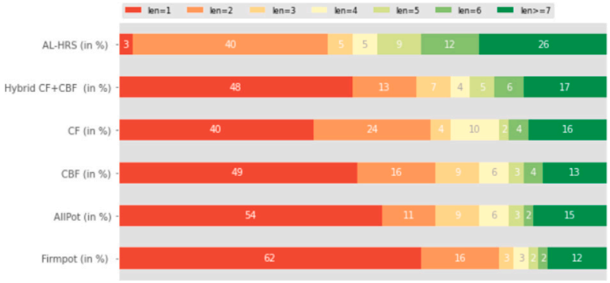


Fig. 5. Comparison of attacker engagement times with recommended vulnerabilities by AL-HRS and existing method.

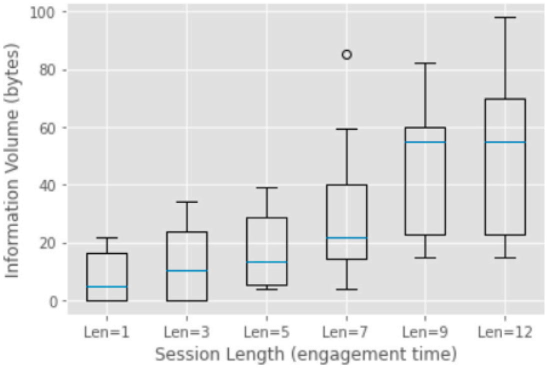


Fig. 6. Correlation between engagement time and volume of information sent by attackers, indicating the effectiveness of the recommended vulnerabilities in extracting valuable intelligence.

4.4.2. *Effectiveness of deception*

Evaluation of engagement times, as illustrated in Fig. 5, provides insight into how long attackers interact with the decoys before discontinuing their activities. Our results show that the deceptive vulnerabilities recommended by AL-HRS successfully engaged 26% of attackers with an average session duration of 7 min. This duration is significantly higher compared to traditional deception methods. Further analysis revealed variability in engagement times: shorter sessions lasted around 2 min, while longer engagements extended up to 12 min. Such variation underscores the system's capability to adapt and cater to different attacker behaviors and strategies, effectively maintaining engagement across a broad spectrum of attack types and intents.

Evaluating engagement time alone does not fully reveal whether our approach is more effective than others in understanding attackers' behaviors. Therefore, a critical aspect of our evaluation focused on the ability to extract actionable intelligence from attackers during their engagement. Our system demonstrated a high detection rate of well-known attacks at approximately 78%, as shown in Fig. 7. In addition, we analyze the volume of information transmitted by attackers during their engagement. As depicted in Fig. 6, there is a clear correlation between the duration of engagement and the volume of information sent by the attacker. This trend is logical; as sessions last, attackers tend to send more specific requests, which in turn increases the volume of information exchanged. This indicates that attackers are more likely to trust and interact with the decoys, suggesting a belief in the authenticity of the recommended vulnerabilities. This relationship underscores the efficacy of our system in engaging attackers and extracting valuable intelligence during these interactions.

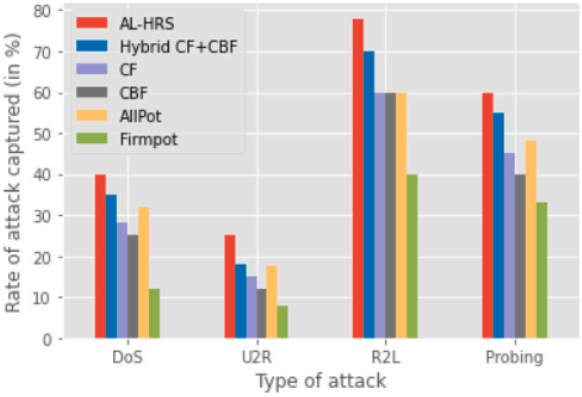


Fig. 7. Detection rate of AL-HRS showing the system's effectiveness in identifying and responding to well-known attack types such as denial of service (DoS), probe, user to root (U2R), and remote to Local (R2L).

Table 5
Comparison of targeting metrics in deception system.

Method	Total number of requests received/total number of request targeting recommended vulnerabilities
AL-HRS	9235/5287
Hybrid CF+CBF	7235/1917
CF only	6235/1087
CBF only	5235/993
AIIPot [24]	6235/987
Firmpot [25]	2896/687

In general, AL-HRS outperformed existing methods by at least 15% in key metrics such as engagement time and detection rates. This superior performance demonstrates the advantages of integrating adaptive learning and hybrid recommendation strategies, particularly in complex and varied testing environments.

4.4.3. *Scalability and response efficiency*

The system maintained a response time of under 2 s in 95% of cases, even as the network scaled up to 100 devices. This responsiveness, coupled with the system's ability to handle increased load without degradation in performance, underscores its scalability and efficiency. Furthermore, AL-HRS successfully mitigated over 50% of advanced persistent threats and zero-day exploits, underlining its ability to adapt to new and emerging threats.

Over a one-month testing period, the system's effectiveness improved by 15%, reflecting its capacity to learn and adapt based on attacker feedback and changing attack patterns. During this period, the system captures 9235 requests with 5287 targeting the recommended vulnerability. This is far better than the non-adaptive hybrid CF+CBF, solely CF, solely CBF and AIIPot [24]. Table 5 shows that while actual vulnerabilities received a significant number of requests, the recommended vulnerabilities attracted a comparably higher number of requests. This indicates that the decoys are effective in diverting attention away from real vulnerabilities. Additionally, it is noteworthy that despite the higher number of requests on recommended vulnerabilities, the number of attackers targeting them is slightly less than those targeting actual vulnerabilities, suggesting effective confusion and misdirection.

4.5. Discussion

The evaluation of AL-HRS has illuminated its strengths and areas for improvement. Notably, the system demonstrated a high detection rate of well-known attacks and was effective in misleading attackers with deceptive vulnerabilities, supporting our goal to enhance IoT security through an innovative deception strategy.

Our AL-HRS achieves higher accuracy due to its integration of both CF and CBF within a dynamic learning framework. Unlike traditional static systems, AL-HRS continuously adapts to new data and attacker behaviors. This adaptability allows it to refine its detection algorithms in real-time, improving its accuracy in identifying and countering threats. Empirical tests have shown that AL-HRS outperforms conventional static systems by dynamically updating its defense mechanisms to respond to evolving threats more effectively.

The significant increase in attacker engagement time with deceptive vulnerabilities corroborates the system's ability to distract and detain attackers effectively. This is further evidenced by the correlation between engagement times and the volume of information exchanged, indicating that attackers perceived the decoys as legitimate targets. These results affirm the system's success in creating convincing and interactive decoys that extend attacker interaction, thereby reducing the likelihood of attacks on real assets.

Despite its achievements, AL-HRS showed less efficacy against complex multi-vector attacks, which are characterized by the simultaneous exploitation of multiple vulnerabilities or the sequential application of diverse attack techniques. These advanced attack scenarios typically require rapid and multifaceted responses, which poses a challenge for our current system configuration. This limitation was particularly noticeable in simulated environments where coordinated attacks combined elements like DDoS distractions with subtler exploit attempts such as SQL injections.

The reduced incidence of successful attacks on actual devices underscores the practical utility of AL-HRS in real-world settings. However, to maintain this effectiveness, ongoing development and optimization of the system are crucial. Enhancing its adaptability to handle new and sophisticated attack vectors will be critical, especially as IoT technologies continue to proliferate and integrate into more complex networks.

Deploying our system within real IoT networks requires meticulous traffic differentiation to prevent misidentification and incorrect routing. We integrate the advanced traffic analysis techniques proposed by Choi et al. [34], utilizing machine learning classifiers to accurately distinguish between legitimate user interactions and potential threat activities based on behavioral patterns and network signatures. Embedded safeguards within our network infrastructure ensure that legitimate traffic is processed seamlessly, while suspicious activities are strategically rerouted to honeypots. Although the model from Choi et al. is not 100% accurate, occasional misidentification of legitimate traffic may occur. To mitigate this, our system is designed to continuously learn from such interactions, refining its recommendations to minimize risks effectively. This adaptive approach ensures that our deceptive defense remains robust without significantly impacting legitimate network operations, thereby preserving the integrity and reliability of network services over time.

5. Conclusion

In this paper, we introduced AL-HRS, an adaptive learning-based hybrid recommender system for IoT security, designed to implement a sophisticated deception strategy. The system's integration of CF and CBF with an adaptive learning mechanism proved highly effective, outperforming traditional non-adaptive hybrid approaches, as well as standalone CF and CBF systems and existing deception systems. The superior performance of AL-HRS was demonstrated through its high precision, recall, and F1 scores, which affirm its effectiveness in accurately identifying and recommending deceptive vulnerabilities. The practical benefits of AL-HRS were highlighted by the increased engagement time with attackers and the high detection rates of simulated attacks, which significantly reduced the number of successful attacks on actual devices. Despite these successes, our evaluation identified challenges in countering complex multi-vector attacks, which involve sophisticated and coordinated strategies that exploit multiple vulnerabilities simultaneously. This limitation underscores the necessity for further research and development to enhance the system's capabilities, ensuring it can anticipate and neutralize evolving cyber threats effectively.

Looking ahead, the field of IoT security is increasingly vital as the proliferation of connected devices continues to rise. Advancing deceptive defense strategies is essential to foster more resilient and adaptive security frameworks. Our research provides a foundational step in this direction, offering significant insight and a robust platform on which future innovations can be based, ensuring the ongoing protection and robustness of IoT environments.

CRediT authorship contribution statement

Volviane Saphir Mfogo: Writing – review & editing, Writing – original draft, Methodology, Formal analysis, Data curation, Conceptualization. **Alain Zemkoho:** Writing – review & editing, Validation, Supervision, Methodology. **Laurent Njilla:** Writing – review & editing, Supervision, Methodology. **Marcellin Nkenlifack:** Writing – review & editing, Supervision. **Charles Kamhoua:** Writing – review & editing, Supervision, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] Claudia Campolo, Giacomo Genovese, Antonio Iera, Antonella Molinaro, Virtualizing AI at the distributed edge towards intelligent IoT applications, J. Sensor Actuat. Netw. 10 (1) (2021) 13.

[2] Sean W. Smith, Securing the internet of things: An ongoing challenge, Computer 53 (6) (2020) 62–66.

[3] Jayashree Mohanty, Sushree Mishra, Sibani Patra, Bibudhendu Pati, Chhabi Rani Panigrahi, IoT security, challenges, and solutions: a review, in: Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2019, Volume 2, Springer, 2021, pp. 493–504.

[4] Yupeng Hou, Junjie Zhang, Zihan Lin, Hongyu Lu, Ruobing Xie, Julian McAuley, Wayne Xin Zhao, Large language models are zero-shot rankers for recommender systems, in: European Conference on Information Retrieval, Springer, 2024, pp. 364–381.

[5] Hamed HaddadPajouh, Ali Dehghantanha, Reza M Parizi, Mohammed Aledhari, Hadis Karimipour, A survey on internet of things security: Requirements, challenges, and solutions, Internet Things 14 (2021) 100129.

[6] Lerina Aversano, Mario Luca Bernardi, Marta Cimitile, Riccardo Pecori, A systematic review on deep learning approaches for IoT security, Comp. Sci. Rev. 40 (2021) 100389.

[7] Rasheed Ahmad, Izzat Alsmadi, Machine learning approaches to IoT security: A systematic literature review, Internet Things 14 (2021) 100365.

[8] Veneta Yosifova, Antoniya Tasheva, Roumen Trifonov, Predicting vulnerability type in common vulnerabilities and exposures (cve) database with machine learning classifiers, in: 2021 12th National Conference with International Participation, ELECTRONICA, IEEE, 2021, pp. 1–6.

[9] Alireza Zohourian, Sajjad Dadkhah, Euclides Carlos Pinto Neto, Hassan Mahdikhani, Priscilla Kyei Danso, Heather Molyneaux, Ali A Ghorbani, IoT zigbee device security: A comprehensive review, Internet Things (2023) 100791.

[10] Maha Ali Allouzi, Javed I. Khan, Identifying and modeling security threats for IoMT edge network using Markov chain and common vulnerability scoring system (CVSS), 2021, arXiv preprint arXiv:2104.11580.

[11] Abiodun Esther Omolara, Abdullah Alabdulatif, Oludare Isaac Abiodun, Moatsum Alawida, Abdulatif Alabdulatif, Humaira Arshad, et al., The internet of things security: A survey encompassing unexplored areas and new insights, Comput. Secur. 112 (2022) 102494.

[12] Mengmeng Ge, Jin-Hee Cho, Dongseong Kim, Gaurav Dixit, Ing-Ray Chen, Proactive defense for internet-of-things: moving target defense with cyberdeception, ACM Trans. Internet Technol. (TOIT) 22 (1) (2021) 1–31.

[13] Rami Puzis, et al., Agro-fake: optimal attack graph obfuscation using fake vulnerabilities, 2019, Accessed [9 May 2024].

[14] Mu Zhu, Ahmed H Anwar, Zelin Wan, Jin-Hee Cho, Charles A Kamhoua, Munindar P Singh, A survey of defensive deception: Approaches using game theory and machine learning, IEEE Commun. Surv. Tutor. 23 (4) (2021) 2460–2493.

[15] Morteza Safaei Pour, Joseph Khoury, Elias Bou-Harb, HoneyComb: A darknet-centric proactive deception technique for curating IoT malware forensic artifacts, in: NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2022, pp. 1–9.

[16] Deepjyoti Roy, Mala Dutta, A systematic review and research perspective on recommender systems, J. Big Data 9 (1) (2022) 59.

[17] Aleksandra Pawlicka, Marek Pawlicki, Rafał Kozik, Ryszard S Choraś, A systematic review of recommender systems and their applications in cybersecurity, Sensors 21 (15) (2021) 5248.

[18] Riya Widayanti, Mochamad Heru Riza Chakim, Chandra Lukita, Untung Rahardja, Ninda Lutfiani, Improving recommender systems using hybrid techniques of collaborative filtering and content-based filtering, J. Appl. Data Sci. 4 (3) (2023) 289–302.

[19] Zhiyan Chen, Jinxin Liu, Yu Shen, Murat Simsek, Burak Kantarci, Hussein T Mouftah, Petar Djukic, Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats, ACM Comput. Surv. 55 (5) (2022) 1–37.

[20] Yuba Raj Siwakoti, Manish Bhurtel, Danda B Rawat, Adam Oest, RC Johnson, Advances in IOT security: Vulnerabilities, enabled criminal services, attacks and countermeasures, IEEE Internet Things J. (2023).

[21] Eryk Schiller, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, Burkhard Stiller, Landscape of IoT security, Comp. Sci. Rev. 44 (2022) 100467.

[22] Iqbal H Sarker, Asif Irshad Khan, Yoosef B Abushark, Fawaz Alsolami, Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions, Mob. Netw. Appl. 28 (1) (2023) 296–312.

[23] Edward A Cranford, Cleotilde Gonzalez, Palvi Aggarwal, Milind Tambe, Sarah Cooney, Christian Lebiere, Towards a cognitive theory of cyber deception, Cogn. Sci. 45 (7) (2021) e13013.

[24] Volviane Saphir Mfogo, Alain Zemkoho, Laurent Njilla, Marcellin Nkenlifack, Charles Kamhoua, AIIPot: Adaptive intelligent-interaction honeypot for IoT devices, in: 2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC, 2023, pp. 1–6.

[25] Moeka Yamamoto, Shohei Kakei, Shoichi Saito, Firmpot: A framework for intelligent-interaction honeypots using firmware of iot devices, in: 2021 Ninth International Symposium on Computing and Networking Workshops, CANDARW, IEEE, 2021, pp. 405–411.

[26] Philip Huff, Kylie McClanahan, Thao Le, Qinghua Li, A recommender system for tracking vulnerabilities, in: Proceedings of the 16th International Conference on Availability, Reliability and Security, 2021, pp. 1–7.

[27] Sherin Eliyas, P. Ranjana, Recommendation systems: Content-based filtering vs collaborative filtering, in: 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE, IEEE, 2022, pp. 1360–1365.

[28] Yassine Afoudi, Mohamed Lazaar, Mohammed Al Achhab, Hybrid recommendation system combined content-based filtering and collaborative prediction using artificial neural network, Simul. Model. Pract. Theory 113 (2021) 102375.

[29] Marek Janiszewski, Anna Felkner, Piotr Lewandowski, Marcin Rytel, Hubert Romanowski, Automatic actionable information processing and trust management towards safer internet of things, Sensors 21 (13) (2021).

[30] Guru Bhandari, Amara Naseer, Leon Moonen, Cvefixes: automated collection of vulnerabilities and their fixes from open-source software, in: Proceedings of the 17th International Conference on Predictive Models and Data Analytics in Software Engineering, 2021, pp. 30–39.

[31] Eitan Altman, Constrained Markov Decision Processes, Routledge, 2021.

[32] Thomas M Moerland, Joost Broekens, Aske Plaat, Catholijn M Jonker, et al., Model-based reinforcement learning: A survey, Found. Trends Mach. Learn. 16 (1) (2023) 1–118.

[33] R. Rengarajan, Shekar Babu, Anomaly detection using user entity behavior analytics and data visualization, in: 2021 8th International Conference on Computing for Sustainable Global Development, INDIACom, IEEE, 2021, pp. 842–847.

[34] Seunghyun Choi, Changgyun Kim, Yong-Shin Kang, Sekyoung Youm, Human behavioral pattern analysis-based anomaly detection system in residential space, J. Supercomput. 77 (2021) 9248–9265.

Volviane Saphir Mfogo is currently pursuing a Ph.D. degree with the Faculty of Science, department of Mathematics and Computer Science, University of Dschang. She is working on Machine learning and Cyber-security under the Game theory and Machine learning for Cyber Deception, Resilience and Agility (GMC-DRA) project, sponsored by the US Army research lab. She is African Master in Machine Intelligence (AMMI), alumni where she obtained a Msc. In Machine Learning sponsored by Facebook and Google. Before joining AMMI, she obtained an MSc. In Mathematics from African Institute for Mathematical Sciences (AIMS Cameroon).

Alain Zemkoho an associate professor in operational research at the School of Mathematical Sciences within the University of Southampton where I am affiliated to the OR Group and CORMSIS. Prior to joining Southampton, I was a Research Fellow at the University of Birmingham and had previously worked as a Research Associate at the Technical University of Freiberg. I am an Alexander von Humboldt Experienced Fellow 2024–2026, a Fellow of the Alan Turing Institute for Data Science and Artificial Intelligence 2019–2023, a Fellow of the Institute of Mathematics & Its Applications, and a Fellow of the Higher Education Academy.

Laurent Njilla joined the Cyber Assurance Branch of the US Air Force Research Laboratory (AFRL), Rome, NY, as a Research Electronics Engineer in 2015. As a researcher, he is responsible for conducting and directing basic research in the area of cyber defense, cyber physical system, cyber resiliency, hardware security, and the application of game theory, category theory, and Blockchain technology. He is the Program Manager of the Center of Excellence (CoE) in Cyber Security for the Historically Black Colleges and Universities & Minorities Institutions (HBCU/MI), and the Program Manager of the Disruptive Information Technology Program at AFRL/RI. He has coauthored over 70 peer-reviewed journal and conference papers with a best paper award. He is a coinventor of 2 patents and 3 patent applications.

Marcellin Julius Nkenlifack is the Head of Mathematics and Computer Science Department, University of Dschang, Cameroon, and a Professor. He received M.A. degrees in Computer Science, followed by Ph.D. in Computer Engineering and Control from National Polytechnic Institute, University of Yaounde I. He had been a visiting researcher at Institut Scientifique et Polytechnique Galilee, Universite de Paris 13 (2001) and SUPELEC - Rennes, France (2003).

Charles A. Kamhoua is a Senior Electronics Engineer at the Network Security Branch of the DEVCOM Army Research Laboratory (ARL) in Adelphi, MD, where he is responsible for conducting and directing basic research in the area of game theory applied to cyber security. Prior to joining the Army Research Laboratory, he was a researcher at the US Air Force Research Laboratory (AFRL), Rome, New York, for 6 years and an educator in different academic institutions for more than 10 years. He has held visiting research positions at the University of Oxford and Harvard University. He has coauthored more than 200 peer-reviewed journal and conference papers that include 5 best paper awards.