Large Language Model-driven Security Assistant for Internet of Things via Chain-of-Thought

Mingfei Zeng, Ming Xie, Xixi Zheng, Chunhai Li, Chuan Zhang, Liehuang Zhu

***Abstract*—The rapid development of Internet of Things (IoT) technology has transformed people's way of life and has a profound impact on both production and daily activities. However, with the rapid advancement of IoT technology, the security of IoT devices has become an unavoidable issue in both research and applications. Although some efforts have been made to detect or mitigate IoT security vulnerabilities, they often struggle to adapt to the complexity of IoT environments, especially when dealing with dynamic security scenarios. How to automatically, efficiently, and accurately understand these vulnerabilities remains a challenge. To address this, we propose an IoT security assistant driven by Large Language Model (LLM), which enhances the LLM's understanding of IoT security vulnerabilities and related threats. The aim of the ICoT method we propose is to enable the LLM to understand security issues by breaking down the various dimensions of security vulnerabilities and generating responses tailored to the user's specific needs and expertise level. By incorporating ICoT, LLM can gradually analyze and reason through complex security scenarios, resulting in more accurate, in-depth, and personalized security recommendations and solutions. Experimental results show that, compared to methods relying solely on LLM, our proposed LLM-driven IoT security assistant significantly improves the understanding of IoT security issues through the ICoT approach and provides personalized solutions based on the user's identity, demonstrating higher accuracy and reliability.**

***Index Terms*—Internet of Things, Chain-of-Thought, Security, Large Language Model.**

I. Introduction

THE rapid development of the Internet of Things (IoT) has profoundly transformed both industrial and everyday life by connecting a wide array of devices and systems, significantly enhancing operational efficiency, convenience, and overall productivity. IoT technologies enable devices to communicate in real time, driving innovations in various sectors such as healthcare, smart homes, transportation, and smart grids [1], [2]. Hundreds of billions of IoT devices have already been integrated into home and industrial environments, fundamentally changing the way people live [3]. However, alongside these advancements, the rapid proliferation of IoT devices also introduces significant security challenges that cannot be overlooked.

As the number of devices interconnected increases, there is a dramatic rise in cyberattacks targeting IoT devices [4]. These attacks exploit vulnerabilities in both the hardware and software of IoT devices, often with the intent of stealing sensitive data, disrupting services, or even gaining unauthorized control over critical systems. Although considerable progress has been made in IoT security research, the complexity of IoT environments characterized by heterogeneous devices, diverse communication protocols, and varying levels of security standards presents ongoing challenges in identifying, understanding, and mitigating vulnerabilities [5]. In such a dynamic and evolving landscape, developing robust solutions to accurately detect and address IoT security issues remains a pressing concern for both researchers and practitioners alike.

Several studies have attempted to detect and analyze IoT vulnerabilities in a traditional way [6]–[8], and with the development of artificial intelligence, some research has leveraged machine learning and deep learning to bring new insights into IoT security [9]–[13]. However, existing methods often rely on predefined rules or static threat models, which are difficult to adapt to the constantly evolving and diverse nature of IoT environments. Additionally, the complexity of IoT systems, involving heterogeneous devices, protocols, and data streams, makes it challenging to provide comprehensive and actionable security insights, particularly when assisting users with different levels of knowledge.

To address these challenges, we propose a LLM-driven Security Assistant that provides personalized and practical vulnerability analysis and solutions for different types of users. Specifically, we introduce the IoT Chain-of-Thought (ICoT), which aims to enhance the LLM's understanding of IoT security vulnerabilities and threats by breaking down the characteristics of security issues and providing personalized security advice based on specific user needs and expertise levels. Extensive experiments have confirmed that ICoT significantly improves the ability to detect and resolve security vulnerabilities in IoT systems, offering a novel solution for strengthening IoT security in an increasingly interconnected world. To summarize, our main contributions are as follows:

- We introduce an innovative IoT security assistant driven by LLMs that improves the understanding of IoT security vulnerabilities and threats, offering personalized responses tailored to users with diverse professional backgrounds.
- Our proposed ICoT method breaks down the characteristics of security vulnerabilities, enabling the LLM to generate more accurate security recommendations for IoT

Mingfei Zeng and Ming Xie are with Guangxi Power Grid Co., Ltd., China. Email: zeng_mf.xt@gx.csg.cn, wolfgangtse@qq.com.

Xixi Zheng, Chuan Zhang, and Liehuang Zhu are with School of Cyberspace Science and Technology, Beijing Institute of Technology. Email: bit-zhengxixi@bit.edu.cn, chuanz@bit.edu.cn, liehuangz@bit.edu.cna.

Chunhai Li is with Guangxi Engineering Research Center of Industrial Internet Security and Blockchain, Guilin University of Electronic Technology. Email: chunhaili@guet.edu.cn.

This work is supported by the National Natural Science Foundation of China (Grant No. 62472032), the Open Foundation of Key Laboratory of Cyberspace Security, Ministry of Education of China (Grant No.KLCS20240209), and the Young Elite Scientists Sponsorship Program by CAST (Grant No. 2023QNRC001).

environments, without the need for task-specific fine-tuning or domain-specific datasets, making it widely applicable to a variety of IoT security scenarios.
- Extensive experimental evaluations demonstrate that ICoT significantly improves the identification and mitigation of IoT security vulnerabilities, outperforming traditional methods in both accuracy and reliability.

II. Related Work

In this section, we introduce some IoT threats, along with a discussion of traditional and LLM-based IoT security-related work, and finally, we present relevant information about CoT.

A. IoT Security Threat and Traditional Methods

IoT provides ubiquitous sensing and computational capabilities [14], having found extensive applications across various domains, including healthcare [15], transportation [16], and industrial systems [17]. It is estimated that the global IoT device population is projected to reach 125 billion by 2030 [18]. However, the exponential growth of IoT devices, coupled with insufficient security measures, leaves IoT systems highly vulnerable to cyberattacks [19], such as botnets [20], ransomware [21], advanced persistent threats (APT) [22], and man-in-the-middle (MITM) [23]. Furthermore, the OWASP Top Ten IoT Security Risks report [24] highlights persistent vulnerabilities in current IoT systems, particularly weak password configurations, firmware vulnerabilities, and unauthorized data access.

To enhance IoT security, researchers have developed various vulnerability detection tools [6]–[8]. Firmalice [6] automates vulnerability identification through an input determinism model. However, its detection capability is limited in scope and ineffective against complex attack scenarios. Traditional approaches targeting embedded systems and their firmware in IoT have increasingly struggled to address the growing sophistication of security threats. Machine learning (ML) and deep learning (DL), with their capacity to process large and diverse datasets and autonomously learn vulnerability patterns, have attracted growing research interest in IoT security protection [9]–[13]. For instance, Shafiq et al. [11] proposed CorrAUC, an ML-based method for detecting malicious IoT traffic. It utilizes AUC metrics to filter relevant features and further applies an ensemble of TOPSIS and Shannon entropy to validate the selected features. According to DL, Vasan et al. [12] introduced the MTHAE model, which combines information gain and OpCode dictionary techniques with hybrid feature selection architectures for IoT malware detection. Despite their advantages in data-driven modeling and automated feature extraction, ML/DL methods still face limitations. Their heavy dependence on data quantity, along with insufficient semantic understanding and contextual reasoning, hinders their ability to provide comprehensive and actionable insights for securing IoT systems.

B. LLM-based Methods for Enhancing IoT Security

LLMs, as advanced neural network architectures, have achieved remarkable breakthroughs in natural language processing. Typically pre-trained on large-scale multimodal datasets comprising text, code, and other data types, LLMs exhibit strong contextual reasoning capabilities and high-quality decision-making performance [25]. Representative models include the Generative Pre-trained Transformer (GPT) series, BERT [26], LLaMA [27], and DeepSeek [28]. Leveraging these advantages, LLMs offer novel technical solutions to address key challenges inherent in IoT, such as data heterogeneity and stringent real-time processing requirements. Through powerful semantic modeling and inference capabilities, LLMs can significantly enhance the understanding and processing efficiency of data streams within IoT systems. Furthermore, the integration of LLMs into resource-constrained environments enables context-aware edge intelligence, allowing IoT systems to better adapt to dynamically changing conditions and improving overall responsiveness and intelligence [29].

As the convergence of LLMs and IoT continues to deepen, increasing research attention has been directed toward their potential in enhancing IoT security tasks, particularly in areas such as vulnerability detection [30]–[32], intrusion prevention [33]–[35], and threat intelligence analysis [36], [37]. For vulnerability detection, Ma et al. [32] proposed mGPTFuzz, the first fuzzing framework specifically designed for vulnerability discovery in Matter-based IoT devices. This tool leverages LLMs to translate human-readable content from the Matter specification into machine-interpretable representations, specifically as finite state machines. Based on a controller-oriented architecture and tailored fuzzing strategies, mGPTFuzz performs black-box fuzz testing on Matter devices to identify potential security vulnerabilities. For intrusion prevention, Ferrag et al. [33] developed SecurityBERT, a network threat detection framework specialized for IoT environments. The system extracts features from network traffic data and employs a BERT-based architecture for model training and fine-tuning. For threat intelligence analysis, Hu et al. [37] devised a method for constructing knowledge graphs from unstructured threat intelligence. By leveraging the few-shot learning capabilities of GPT, the framework performs data annotation and augmentation to build a fine-tuning dataset, which is then used to enable automated analysis of textual threat intelligence through the fine-tuned model.

C. Chain-of-Thought

CoT is a reasoning paradigm that enhances the reasoning capabilities of LLMs by prompting them to generate intermediate reasoning steps before arriving at a final answer [38]. Unlike traditional approaches that directly respond to a task, CoT emphasizes a progressive process by decomposing complex problems into a sequence of logically connected sub-problems, thereby mimicking human reasoning. This approach not only improves accuracy in tasks involving arithmetic or logical reasoning but also ensures enhanced interpretability of the decision-making process.

Building upon CoT, Yao et al. [39] introduced the Tree-of-Thought (ToT) method, which leverages tree search to expand the reasoning space and discover more optimal reasoning paths that may be overlooked by CoT. However, this method incurs significant additional inference costs. To mitigate this

limitation, Zhang et al. [40] further proposed the Chain-of-Preference Optimization (CPO). It utilizes the tree structures generated by ToT to collect preference data at each reasoning step and applies the Direct Preference Optimization (DPO) algorithm to fine-tune the LLM. As a result, the model is guided to select superior reasoning paths while effectively avoiding the high computational overhead associated with ToT.

III. IoT SECURITY ASSISTANT

The increasing complexity and diversity of IoT systems make protecting these environments more challenging than ever before. IoT devices, ranging from smart appliances to industrial sensors, often operate in heterogeneous environments with varying security requirements. Traditional security solutions struggle to adapt to these dynamic systems, making the need for smarter and more adaptable security assistants even more apparent.

To address this issue, we propose an IoT security assistant driven by LLMs, enhanced through the ICoT process. In this section, we first introduce the design goals of the IoT security assistant, followed by an overview of the basic system architecture.

A. Design Goals

The design goals of our IoT security assistant can be broken down into the following subgoals:

1) *Improved Understanding of IoT Security Threats:* The primary goal is to enhance the LLM's ability to comprehend the nuances of IoT security vulnerabilities and threats. Traditional security models often lack the flexibility to address the diverse range of security issues faced by IoT devices. By employing ICoT, our system can reason step-by-step through security scenarios, allowing for a more comprehensive understanding of potential vulnerabilities.
2) *Context-Aware Security Recommendations:* Different IoT environments require different security measures. Our system aims to generate security recommendations that are not only accurate, but also tailored to the specific needs of the user and the IoT system in question. Specifically, we generate correct and personalized security recommendations by breaking down the characteristics of security vulnerabilities and the features of the user.
3) *Scalability and Flexibility:* IoT environments are constantly evolving, with new devices and technologies added regularly. Therefore, our security assistant is designed to scale and adapt to new IoT systems without requiring extensive retraining or task-specific fine-tuning. The ICoT method ensures that the assistant can handle various security challenges of the IoT in different contexts.
4) *Ease of Use and Integration:* To ensure broad adoption and utility, the system is designed to be user-friendly and easy to integrate into existing IoT networks. The security assistant should provide clear, actionable advice that can be understood by users with varying levels of expertise.

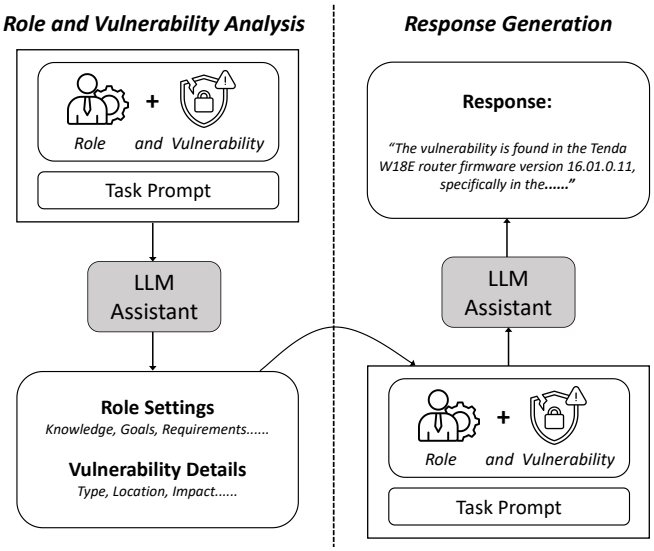

Fig. 1. System architecture.

B. System Architecture

The general workflow of the IoT security assistant is shown in Fig. 1. The LLM plays two roles in this process. First, it analyzes the user's characteristics based on the initial input, such as the user's knowledge level, goals, and requirements, while also analyzing the characteristics of the vulnerability, clarifying the type, location, and impact of the vulnerability. Second, it serves as the model that generates human-readable security recommendations. After the initial processing, the LLM, with the restructured prompt, generates context-aware and actionable advice based on the professional background and specific needs of the user. The LLM is seamlessly integrated with the CoT engine, ensuring that the reasoning process produces relevant and accurate security solutions.

Specifically, ICoT first conducts a detailed analysis of the role and vulnerability inputs and outputs certain feature values. During the second inference of the model, the first output is used as part of the input to assist in the reasoning. This enables the system to consider factors such as device interconnectivity, communication protocols, and operational environments, allowing for reasoning specific to IoT security scenarios. This module ensures that the assistant's reasoning is both relevant and effective within the context of IoT systems.

Together, the LLM and ICoT form a powerful, intelligent IoT security assistant capable of providing effective security support in various IoT environments. The system is adaptive and scalable, requiring no specific models or fine-tuning, ensuring its effectiveness in the dynamic and constantly evolving IoT ecosystem.

IV. IoT CHAIN-OF-THOUGHT

In this section, we introduce ICoT, which enhances the capabilities of LLMs to analyze, understand, and mitigate vulnerabilities in IoT devices. By leveraging a systematic reasoning process, ICoT helps LLMs produce more accurate and context-aware security assessments and recommendations for IoT vulnerabilities.

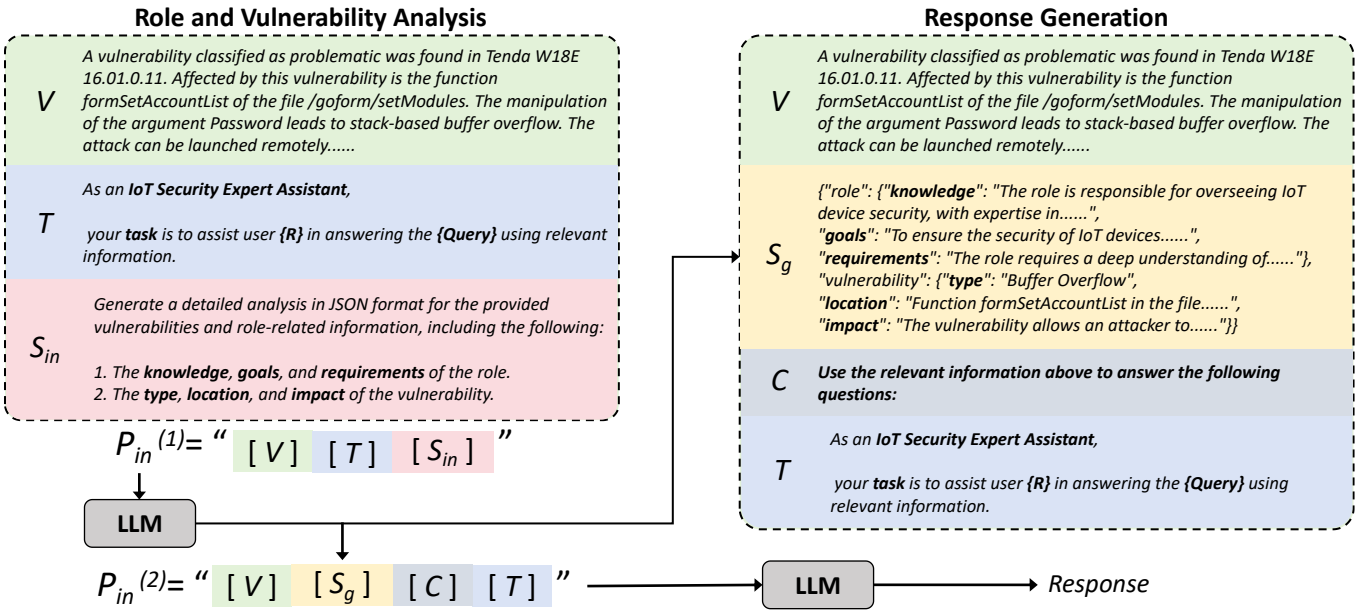

Fig. 2. Full prompt example of ICoT.

A. Preliminaries

The LLM is an advanced and highly sophisticated model specifically designed to process textual input and generate coherent, contextually appropriate responses. When presented with an input prompt P_{in}, which could be in the form of a question, statement, or instruction, the LLM systematically processes this text through multiple transformer-based layers to produce an output response R. This process involves complex interactions between layers that help the model understand and generate human-like text.

Formally, the LLM can be represented as a mathematical function $f_\theta(\cdot)$, where θ represents the parameters that define the model's architecture. This function maps the given input prompt to a corresponding output response, as illustrated in the following equation:

$$R = f_\theta(P_{in}) \tag{1}$$

In this context, the input prompt P_{in} is tokenized, meaning it is converted into smaller, discrete units, and then embedded into a high-dimensional space. This embedding allows the model to capture both the semantic and syntactic relationships present in the text, enabling it to understand the meaning and structure of the input. The architecture of the model and the pre-training methods used to train the parameters θ may differ across various LLM implementations. However, the core framework and the fundamental approach remain consistent, with a focus on processing and generating natural language.

Our proposed method, ICoT, introduces a novel approach that does not require any fine-tuning or direct access to the model's underlying parameters θ. Instead, ICoT leverages the inherent reasoning capabilities that are already built into the LLM by using carefully crafted prompts. This makes ICoT a practical and highly efficient technique, as it allows for optimal utilization of the model's pre-existing reasoning power without the need for additional adjustments or retraining.

B. Role and Vulnerability Analysis

As shown in Fig. 2, ICoT integrates the CoT framework into the IoT security context by applying a step-by-step reasoning approach to vulnerability analysis. This method ensures that the model considers a variety of factors related to the IoT device, such as its role in the network, the nature and severity of the vulnerability, and the potential consequences of an attack. By analyzing the vulnerability in this comprehensive manner, the system can generate more reliable, context-aware security advice that helps users address potential risks effectively.

The first step in the ICoT process involves analyzing both the background of the user, R, and the characteristics of the vulnerability. This dual analysis ensures that the system's response is accurate, relevant, and specifically tailored to the needs and expertise of the user. This process can be formalized as:

$$P_{in}^{(1)} = \text{“}[V][T][S_{in}]\text{”} \tag{2}$$

where $P_{in}^{(1)}$ represents the input for this iteration, V is the vulnerability description, T is the user's role and query, and S_{in} is the analysis prompt.

For example, the following is a description of a vulnerability: “*A vulnerability classified as problematic was found in Tenda W18E 16.01.0.11. Affected by this vulnerability is the function formSetAccountList in the file /goform/setModules. The manipulation of the argument Password leads to a stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Shenzhen Tenda Technology Co., Ltd. of W18E has an out-of-bounds write vulnerability in the firmware. Service operation interruption (DoS) may occur.*”

ICoT analyzes this vulnerability by considering the following factors:

- *Vulnerability Type:* In this case, the vulnerability is identified as a buffer overflow, a common and critical issue in IoT systems.
- *Location:* The vulnerability is found within a specific function in the device's firmware, which helps to pinpoint where the issue lies.
- *Impact:* The remote execution of arbitrary code or a denial of service (DoS) attack due to a system crash may result from exploiting this vulnerability.

In this process, user analysis also plays a crucial role alongside device and vulnerability analysis. The system must evaluate the user's role and level of expertise to generate responses that are not only technically accurate but also comprehensible. This requires consideration of the user's specific query $Query$. Important aspects of user analysis include:

- *User Knowledge:* The system assesses the user's familiarity with IoT security issues. For instance, a network administrator might require in-depth technical details, whereas a general user may only need basic, actionable steps to mitigate risks.
- *User Goals:* The assistant takes into account the user's primary objectives, such as securing a network, preventing unauthorized access, or minimizing system downtime. Understanding these goals helps the system prioritize the most important aspects of the vulnerability that need to be addressed.
- *User Requirements:* The system also evaluates the user's practical constraints, such as available technical resources for patching devices, whether they are working in a critical production environment where downtime is unacceptable, or if a temporary solution is needed before a permanent fix can be applied. This part is specifically determined by $Query$.

Certainly, the analysis of vulnerabilities and users is not limited to the aspects mentioned above. Given the variety of vulnerabilities found in IoT systems, in addition to the type, location, and impact, other characteristics can also be considered for analysis. For example, factors such as the severity of the vulnerability, the attack vector (e.g., remote or local exploitation), and the likelihood of exploitation based on known threat intelligence can all provide additional insights. Additionally, vulnerabilities may have different levels of exploitability depending on the environment in which the device operates, such as whether it is in a private network or exposed to the public internet.

User analysis follows a similar approach. Apart from understanding the user's technical expertise and goals, more granular user characteristics can be considered. For instance, the user's level of familiarity with specific IoT devices, their previous experience with security incidents, or even their role within an organization can all influence how the system generates a response. In certain cases, users might even define role templates in advance, allowing them to directly input user characteristics into the second phase of the process. This approach eliminates the need for the initial analysis round, making the system more efficient and reducing the processing time required to generate a response. While the current approach involves an initial round of vulnerability and user analysis, ICoT is flexible enough to accommodate a more streamlined process where predefined user profiles are directly input into the response generation phase. This flexibility allows for faster, more targeted recommendations.

The detailed analysis of both the vulnerability and the user is essential for the next step in the ICoT process. The system generates a tailored response based on both the technical details of the vulnerability and the user's specific context, expertise, and requirements. By incorporating this dual analysis approach, ICoT ensures that the response is not only technically precise but also actionable and relevant to the user's particular situation. Consequently, the LLM generates a JSON format S_g that encapsulates both user and vulnerability characteristics, as follows:

$$S_g = f_\theta(P_{in}^{(1)}) \tag{3}$$

C. Response Generation

Once the role and vulnerability have been thoroughly analyzed, the next phase of the ICoT process focuses on generating specific responses. The input for this phase, $P_{in}^{(2)}$, can be formally represented as:

$$P_{in}^{(2)} = \text{“}[V][S_g][C][T]\text{”} \tag{4}$$

Here, S_g represents the output from the first phase, which includes the results of both the vulnerability and user analysis. The C component provides a brief instruction to the LLM, prompting it to consider the provided context. This is explicitly given as: “*Use the relevant information above to answer the following questions:*”. This ensures that the model integrates all relevant data when generating its response.

This phase is pivotal because it bridges the reasoning process and translates it into practical, actionable advice for the user. By leveraging the insights from the vulnerability and user analysis, the system can now generate customized recommendations. These responses include:

1) *Actionable recommendations:* These responses could suggest specific steps, such as patching the identified vulnerability, disabling the affected features, or implementing compensatory security measures to mitigate the risk. The goal is to provide immediate and practical actions that the user can take to address the vulnerability.
2) *Security best practices:* Beyond addressing the current vulnerability, the system can also recommend general security practices to help prevent future risks. These might include strategies such as ensuring proper user input sanitization, validating data rigorously, or employing encryption to secure sensitive communications.
3) *Context-aware responses:* The advice given will vary depending on the user's role and technical expertise. For a general user, the response may be simpler, recommending easy-to-follow actions like updating firmware or changing passwords. For a developer or network administrator, the suggestions might include more technical measures such as deploying specific patches or modifying the system's code to prevent the vulnerability from reappearing.

By incorporating role-specific context and a detailed understanding of security threats, the system ensures that the advice it provides is both precise and highly relevant to the user's situation. This context-aware approach guarantees that the responses are not only actionable but also appropriately tailored to the user's capabilities and needs. Thus, the LLM generates the final response R for the vulnerability, user, and prompt, as follows:

$$R = f_\theta(P_{in}^{(2)}) \tag{5}$$

V. Experiments

We applied the ICoT method to four popular LLMs: GPT-4o [41], GPT-4o-mini, DeepSeek-R1 [42], and DeepSeek-V3 [28]. Our primary goal is to determine whether ICoT can effectively generalize and enhance the capabilities of state-of-the-art LLMs in handling IoT security issues.

A. Setup

Dataset. We have gathered two types of datasets related to IoT security and threats. The first, VARIoT Vulnerabilities [43], compiles a collection of known vulnerabilities in IoT devices, along with detailed descriptions of the associated risks. The second, VARIoT Exploits [43], focuses on exploitations targeting IoT devices, providing insights into these vulnerabilities from the perspective of attackers.

Model. We connect four popular LLMs via APIs to serve as the foundation for our IoT security assistant:

1) *GPT-4o:* Developed by OpenAI, GPT-4o is a multimodal model that excels in natural language understanding and generation. It supports text, image, and audio inputs, making it suitable for diverse applications such as voice assistants and real-time translation.
2) *GPT-4o-mini:* GPT-4o-mini is a more compact and cost-effective version of GPT-4o. It offers a balance between performance and efficiency, making it ideal for integration into services with high API call volumes.
3) *DeepSeek-R1:* A Chinese-developed model by DeepSeek, DeepSeek-R1 is optimized for reasoning tasks such as mathematics, code generation, and logical inference. It employs reinforcement learning techniques to enhance its reasoning capabilities.
4) *DeepSeek-V3:* DeepSeek-V3 is a general-purpose model that performs well across various natural language processing tasks. It utilizes a mixture-of-experts architecture to balance performance and computational efficiency.

B. Implementation Details

Although there is a substantial amount of research on IoT security, there is still a lack of publicly available labeled datasets for IoT security vulnerabilities and threat analysis. To evaluate the effectiveness of our ICoT method, we compared the outputs generated by ICoT with those produced by an LLM that does not include the IoT-specific reasoning steps provided by our Chain-of-Thought approach. To assess the quality of the generated answers, we used an independent LLM as an evaluator (fixed as GPT-4o) and measured the results based on five metrics: Accuracy, Relevance, Detail, Technicality, and Friendliness, which are defined as follows:

1) *Accuracy:* The correctness of the answer, ensuring that it aligns with established IoT security principles and accurately addresses the described vulnerabilities or threats.
2) *Relevance:* The extent to which the answer directly addresses the specific question posed by the IoT security scenario and meets the user's needs, considering their professional backgrounds and context.
3) *Detail:* The level of detail provided in the answer, including how well the answer elaborates on the issue and offers a thorough explanation of the security implications.
4) *Technicality:* The response should demonstrate a deep understanding of IoT technologies and their security implications, particularly in relation to IoT protocols, standards, and security measures, ensuring the accuracy and appropriateness of the technical language used.
5) *Friendliness:* The ease of understanding of the answer and its practical value to the user. This includes how well the response translates technical information into actionable security steps or solutions that are tailored to the user's personalized context.

The scores for all five metrics are fixed within the range of [0, 5], with 5 representing the highest quality. The evaluator receives the answers from both ICoT and the LLM-only approach at the same time, ensuring a uniform assessment of both response sets. This approach minimizes the impact of any inherent randomness in the LLM outputs, allowing for a fair and unbiased comparison between the two models [3]. The evaluation framework is shown in Fig. 3.

> ***Task***: *You are an IoT security expert. Please evaluate the following answers.*
>
> ***Answer***:
> *1. ICoT: {Answer_1}*
> *2. LLM only: {Answer_2}*
>
> ***Instructions***:
> *1. Metrics: Descriptions regarding Reliability, Relevance, Detail, Technicality, and User Friendliness.*
> *2. Scores: Provide a score for each answer based on the above metrics. The score range should be from 0 to 5, with 5 being the highest and 0 being the lowest.*

Fig. 3. The evaluation template.

C. Main Results

As shown in Table I, ICoT enhances the performance of LLMs in the field of IoT security. ICoT demonstrates notable improvements across three user roles: General User, Developer, and Technical Officer. Moreover, the personalized responses generated by ICoT lead to increased user friendliness and relevance of the recommendations. However, not all improvements are significant. In addition to the inherent nature

TABLE I
COMPARISON OF ICOT WITH LLM ONLY METHOD.

Role	Metric	GPT-4o		GPT-4o-mini		DeepSeek-V3		DeepSeek-R1	
		ICoT	LLM only	**ICoT**	LLM only	**ICoT**	LLM only	**ICoT**	LLM only
General User	Reliability	4.61(+0.08)	4.53	4.67(+0.39)	4.28	4.77(+0.05)	4.72	4.42(+0.47)	3.95
	Relevance	4.20(+0.14)	4.06	4.34(+0.84)	3.50	4.98(+0.99)	3.99	4.94(+0.14)	4.80
	Detail	4.37(+0.37)	4.00	4.20(+0.10)	4.10	4.81(+0.79)	4.02	4.31(+0.48)	3.83
	Technicality	4.47(+0.81)	3.66	4.43(+0.88)	3.55	4.96(+0.25)	4.71	4.65(+0.31)	4.34
	Friendliness	4.72(+0.09)	4.63	4.04(+0.60)	3.44	4.93(+0.55)	4.38	4.77(+0.80)	3.97
Developer	Reliability	4.27(+0.74)	3.53	4.50(+0.90)	3.60	4.75(+0.62)	4.13	4.68(+0.93)	3.75
	Relevance	4.36(+0.66)	3.70	4.71(+0.10)	4.61	4.28(+0.61)	3.67	4.03(+0.95)	3.08
	Detail	4.35(+0.47)	3.88	4.37(+0.84)	3.53	4.09(+0.74)	3.35	4.43(+0.77)	3.3.66
	Technicality	4.80(+0.65)	4.15	4.31(+0.34)	3.97	4.52(+0.31)	4.21	4.41(+0.94)	3.47
	Friendliness	4.48(+0.62)	3.86	4.16(+0.99)	3.17	3.86(+0.25)	3.61	4.48(+0.18)	4.30
Technical Officer	Reliability	4.52(+0.08)	4.44	4.23(+0.67)	3.56	4.29(+0.27)	4.02	4.36(+0.21)	4.15
	Relevance	4.53(+0.27)	4.26	3.97(+0.40)	3.57	4.43(+0.47)	3.96	4.66(+0.15)	4.51
	Detail	4.87(+0.05)	4.82	4.02(+0.34)	3.68	4.65(+0.11)	4.54	4.18(+0.24)	3.94
	Technicality	4.06(+0.08)	3.98	4.06(+0.21)	3.85	3.80(+0.73)	3.07	4.69(+0.62)	4.07
	Friendliness	4.59(+0.42)	4.17	4.33(+0.11)	4.22	4.99(+0.44)	4.55	4.95(+0.38)	4.57

of the vulnerability descriptions themselves, one possible reason for this is that ICoT sometimes encourages the LLM to generate excessive redundant information, which may diminish the overall clarity or conciseness of the responses.

D. Further Analysis

In addition to the inherent nature of the vulnerability descriptions themselves, one possible reason for the lack of significant improvement in certain cases is that ICoT sometimes encourages the LLM to generate excessive redundant information. This redundancy can negatively impact the clarity and conciseness of the responses, making them less efficient and harder for the user to interpret. While the addition of more context might seem beneficial, it can overwhelm the user with unnecessary details, particularly when concise and actionable advice is needed.

Furthermore, LLMs, despite their powerful reasoning capabilities, are not immune to hallucination—a phenomenon where the model generates information that is plausible-sounding but fabricated. In the case of IoT security, hallucinated content could include incorrect security recommendations or unverified details about vulnerabilities. Such errors can be especially harmful in the context of security analysis, where inaccurate advice could lead to improper mitigation measures or overlooked threats.

While the CoT approach enhances the reasoning process by breaking down problems step by step, it is not always foolproof. CoT is reliant on the model's internal understanding of the problem, which, despite being structured, may still lead to unreliable conclusions in certain situations [44]. The reasoning process may become convoluted or inconsistent when the model struggles with particularly complex or poorly defined vulnerabilities, leading to incorrect or incomplete security assessments.

The presence of redundant information, hallucinations, and inconsistencies in reasoning illustrates the ongoing challenges in applying LLMs to real-world security scenarios. Tackling these issues is essential for enhancing the reliability and performance of ICoT and similar systems in the realm of IoT security.

E. Scalability

Although only three user roles are used in the experiment, we do not restrict the specific identity of the user in practice. Users can even import their own identity templates (during the second input). Similarly, we do not set a fixed number of characteristics to analyze the vulnerabilities; users can adjust this themselves. From various perspectives, ICoT offers a high level of scalability.

VI. DISCUSSION

In this section, we discuss the implications, challenges, and future directions of the ICoT method in the context of IoT security. The ICoT method represents a significant step forward in understanding and addressing IoT security vulnerabilities, but several aspects warrant further exploration.

A. Impact on the IoT Security Field

With the widespread adoption of IoT devices, the security challenges have become increasingly significant, posing major threats to global cybersecurity. The ICoT method proposed in this paper enhances the performance of LLMs in analyzing IoT security vulnerabilities by introducing the CoT reasoning mechanism. Compared to traditional vulnerability detection and response methods, ICoT provides more accurate and in-depth security analysis, especially in handling complex vulnerabilities and dynamic security threats.

The impact of ICoT on the IoT security field can be summarized in several key aspects:

1) *Improved Vulnerability Identification Accuracy:* Traditional vulnerability detection tools often rely on static rules or pattern matching, which can miss emerging vulnerabilities or complex attack patterns. The ICoT method, through step-by-step reasoning, provides a more comprehensive identification of vulnerabilities and potential risks, leading to more reliable security assessments.

2) *Automated Security Response:* ICoT can generate customized security recommendations based on different devices' roles and vulnerability types. This automation reduces the need for manual intervention and significantly enhances the efficiency of security management.
3) *Cross-Domain Application Potential:* While the focus of this paper is IoT security, the ICoT method can also be extended to other security domains, such as Industrial Control Systems (ICS), smart grids, and smart home security.

B. Challenges and Limitations

Although the ICoT method performs well both theoretically and in experiments, it still faces several challenges and limitations in practical applications:

1) *Diversity and Heterogeneity of IoT Devices:* IoT devices come in many varieties, each with different hardware architectures, firmware versions, and security configurations. The reasoning process in ICoT needs to be adapted for different devices, placing high demands on the model's generalization ability. Some devices may lack sufficient security information or fail to release timely patches, making vulnerability analysis more difficult.
2) *Incomplete Vulnerability Data:* IoT device security vulnerability information is often scattered and updated slowly, meaning ICoT may not have access to the latest vulnerability data. Additionally, descriptions of vulnerabilities and their remediation methods may differ between manufacturers, which can make the model less effective in addressing new vulnerabilities.
3) *Inference Efficiency and Real-Time Performance:* While ICoT provides powerful reasoning capabilities, large-scale vulnerability detection and inference tasks can impose significant computational demands. Especially in resource-constrained IoT environments, the efficiency and response time of the inference process could become a performance bottleneck.
4) *Security and Privacy Concerns:* While ICoT can improve security, the large-scale deployment of such systems may involve user privacy and data security issues. In particular, when dealing with sensitive data, ensuring the privacy and security of information remains a challenge that needs to be addressed [45], [46].

C. Future Work

The ICoT method provides a new framework for IoT security analysis, but many avenues for further research and improvement remain:

1) Currently, ICoT is mainly applied to common IoT devices and protocols. Future research can extend ICoT to include more types of IoT devices and communication protocols, such as Low Power Wide Area Network (LPWAN) devices, Industrial IoT (IIoT) devices, etc., to improve its applicability and generalizability.
2) To address the rapid changes in IoT environments and the emergence of new vulnerabilities, the ICoT system needs to further enhance its adaptability, enabling automatic adjustment of reasoning strategies and response plans to deal with new security threats. This may involve online learning or incremental training to continuously optimize the model.
3) Future work can explore integrating more types of sensor data, network traffic information, and system logs into ICoT, further improving its ability to recognize and respond to complex security scenarios. For example, combining visual, audio, and environmental data can enhance the model's capacity for multimodal security analysis.
4) To accommodate large-scale IoT networks, ICoT needs to further optimize its inference efficiency, especially in resource-constrained IoT devices. Research into reducing computational and storage requirements while maintaining high accuracy will be key to enhancing the application potential of this technology.
5) With the widespread deployment of ICoT, safeguarding data security and privacy will be an important research direction. Developing privacy-preserving inference mechanisms and ensuring that IoT security assistants do not leak user privacy while processing sensitive data will help increase user trust in this technology.

VII. Conclusion

In this paper, we introduced an IoT security assistant powered by LLM and enhanced through the ICoT process. Through the ICoT we proposed, the LLM is better equipped to understand and address the complexity of IoT security vulnerabilities, providing more accurate, context-aware security recommendations that align with the user's personalized needs. Specifically, ICoT breaks down the vulnerability and user characteristics through a two-stage analysis to generate more effective security advice. Experimental results show that our approach significantly enhances the ability to analyze vulnerabilities and mitigate security threats, without requiring additional training or fine-tuning. Our system not only improves the LLM's capabilities in the field of IoT security, but also offers a new framework for integrating structured reasoning into large-scale security applications. Future work will explore further optimization of the ICoT process and expand the system's application to a broader range of IoT security challenges, ultimately providing stronger and more efficient security solutions for the rapidly growing IoT ecosystem.

References

[1] A. Al-Ali, R. Gupta, I. Zualkernan, and S. K. Das, "Role of iot technologies in big data management systems: A review and smart grid case study," *Pervasive and Mobile Computing*, p. 101905, 2024.
[2] Z. Zhang, M. Liu, M. Sun, R. Deng, P. Cheng, D. Niyato, M.-Y. Chow, and J. Chen, "Vulnerability of machine learning approaches applied in iot-based smart grid: A review," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 18 951–18 975, 2024.
[3] Y. Dong, Y. L. Aung, S. Chattopadhyay, and J. Zhou, "Chatiot: Large language model-based security assistant for internet of things with retrieval-augmented generation," *arXiv preprint arXiv:2502.09896*, 2025.

[4] M. L. Mutleg, A. M. Mahmood, and M. M. J. Al-Nayar, "A comprehensive review of cyber-attacks targeting iot systems and their security measures." *International Journal of Safety & Security Engineering*, vol. 14, no. 4, 2024.

[5] S. S. Mahadik, P. M. Pawar, and R. Muthalagu, "Heterogeneous iot (hetiot) security: techniques, challenges and open issues," *Multimedia Tools and Applications*, vol. 83, no. 12, pp. 35 371–35 412, 2024.

[6] Y. Shoshitaishvili, R. Wang, C. Hauser, C. Kruegel, and G. Vigna, "Firmalice-automatic detection of authentication bypass vulnerabilities in binary firmware." in *Proceedings of the 22nd Annual Network and Distributed System Security Symposium*, 2015, doi:10.14722/ndss.2015.23294.

[7] N. Corteggiani, G. Camurati, and A. Francillon, "Inception: System-wide security testing of real-world embedded systems software," in *27th USENIX security symposium*, 2018, pp. 309–326.

[8] Y. Zheng, A. Davanian, H. Yin, C. Song, H. Zhu, and L. Sun, "Firm-afl: High-throughput greybox fuzzing of iot firmware via augmented process emulation," in *28th USENIX Security Symposium*, 2019, pp. 1099–1114.

[9] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[10] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in iot security: Current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020.

[11] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "Corrauc: a malicious bot-iot traffic detection method in iot network using machine-learning techniques," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3242–3254, 2020.

[12] D. Vasan, M. Alazab, S. Venkatraman, J. Akram, and Z. Qin, "Mthael: Cross-architecture iot malware detection based on neural network advanced ensemble learning," *IEEE Transactions on Computers*, vol. 69, no. 11, pp. 1654–1667, 2020.

[13] R. Chaganti, V. Ravi, and T. D. Pham, "Deep learning based cross architecture internet of things malware detection and classification," *Computers & Security*, vol. 120, p. 102779, 2022.

[14] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021.

[15] A. Balasundaram, S. Routray, A. Prabu, P. Krishnan, P. P. Malla, and M. Maiti, "Internet of things (iot)-based smart healthcare system for efficient diagnostics of health parameters of patients in emergency care," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18 563–18 570, 2023.

[16] Y. Song, F. R. Yu, L. Zhou, X. Yang, and Z. He, "Applications of the internet of things (iot) in smart logistics: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4250–4274, 2020.

[17] O. Peter, A. Pradhan, and C. Mbohwa, "Industrial internet of things (iiot): opportunities, challenges, and requirements in manufacturing businesses in emerging economies," *Procedia Computer Science*, vol. 217, pp. 856–865, 2023.

[18] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1759–1799, 2021.

[19] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of iot security," *Computer Science Review*, vol. 44, p. 100467, 2022.

[20] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[21] I. Yaqoob, E. Ahmed, M. H. ur Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, and M. Guizani, "The rise of ransomware and emerging security challenges in the internet of things," *Computer Networks*, vol. 129, pp. 444–458, 2017.

[22] Z. Chen, J. Liu, Y. Shen, M. Simsek, B. Kantarci, H. T. Mouftah, and P. Djukic, "Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats," *ACM Computing Surveys*, vol. 55, no. 5, pp. 1–37, 2022.

[23] O. Salem, K. Alsubhi, A. Shaafi, M. Gheryani, A. Mehaoua, and R. Boutaba, "Man-in-the-middle attack mitigation in internet of medical things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2053–2062, 2021.

[24] P. Ferrara, A. K. Mandal, A. Cortesi, and F. Spoto, "Static analysis for discovering iot vulnerabilities," *International Journal on Software Tools for Technology Transfer*, vol. 23, no. 1, pp. 71–88, 2021.

[25] İ. Kök, O. Demirci, and S. Özdemir, "When iot meet llms: Applications and challenges," in *2024 IEEE International Conference on Big Data*. IEEE, 2024, pp. 7075–7084.

[26] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," in *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*, 2019, pp. 4171–4186.

[27] H. Touvron, T. Lavril, G. Izacard, X. Martinet, M.-A. Lachaux, T. Lacroix, B. Rozière, N. Goyal, E. Hambro, F. Azhar *et al.*, "Llama: Open and efficient foundation language models," *arXiv preprint arXiv:2302.13971*, 2023.

[28] A. Liu, B. Feng, B. Xue, B. Wang, B. Wu, C. Lu, C. Zhao, C. Deng, C. Zhang, C. Ruan *et al.*, "Deepseek-v3 technical report," *arXiv preprint arXiv:2412.19437*, 2024.

[29] Y. L. Aung, I. Christian, Y. Dong, X. Ye, S. Chattopadhyay, and J. Zhou, "Generative ai for internet of things security: Challenges and opportunities," *arXiv preprint arXiv:2502.08886*, 2025.

[30] J. Wang, L. Yu, and X. Luo, "Llmif: Augmented large language model for fuzzing iot devices," in *2024 IEEE Symposium on Security and Privacy*. IEEE, 2024, pp. 881–896.

[31] R. Meng, M. Mirchev, M. Böhme, and A. Roychoudhury, "Large language model guided protocol fuzzing," in *Proceedings of the 31st Annual Network and Distributed System Security Symposium*, vol. 2024, 2024.

[32] X. Ma, L. Luo, and Q. Zeng, "From one thousand pages of specification to unveiling hidden bugs: Large language model assisted fuzzing of matter iot devices," in *33rd USENIX Security Symposium*, 2024, pp. 4783–4800.

[33] M. A. Ferrag, M. Ndhlovu, N. Tihanyi, L. C. Cordeiro, M. Debbah, T. Lestable, and N. S. Thandi, "Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices," *IEEE Access*, vol. 12, pp. 23 733–23 750, 2024.

[34] Y. Li, Z. Xiang, N. D. Bastian, D. Song, and B. Li, "Ids-agent: An llm agent for explainable intrusion detection in iot networks," in *NeurIPS 2024 Workshop on Open-World Agents*, 2024.

[35] E. Nwafor, U. Baskota, M. S. Parwez, J. Blackstone, and H. Olufowobi, "Evaluating large language models for enhanced intrusion detection in internet of things networks," in *GLOBECOM 2024-2024 IEEE Global Communications Conference*. IEEE, 2024, pp. 3358–3363.

[36] S. M. Hasan, A. M. Alotaibi, S. Talukder, and A. R. Shahid, "Distributed threat intelligence at the edge devices: A large language model-driven approach," in *2024 IEEE 48th Annual Computers, Software, and Applications Conference*. IEEE, 2024, pp. 1496–1497.

[37] Y. Hu, F. Zou, J. Han, X. Sun, and Y. Wang, "Llm-tikg: Threat intelligence knowledge graph construction utilizing large language model," *Computers & Security*, vol. 145, p. 103999, 2024.

[38] J. Wei, X. Wang, D. Schuurmans, M. Bosma, F. Xia, E. Chi, Q. V. Le, D. Zhou *et al.*, "Chain-of-thought prompting elicits reasoning in large language models," *Advances in Neural Information Processing Systems*, vol. 35, pp. 24 824–24 837, 2022.

[39] S. Yao, D. Yu, J. Zhao, I. Shafran, T. Griffiths, Y. Cao, and K. Narasimhan, "Tree of thoughts: Deliberate problem solving with large language models," *Advances in Neural Information Processing Systems*, vol. 36, pp. 11 809–11 822, 2023.

[40] X. Zhang, C. Du, T. Pang, Q. Liu, W. Gao, and M. Lin, "Chain of preference optimization: Improving chain-of-thought reasoning in llms," *Advances in Neural Information Processing Systems*, vol. 37, pp. 333–356, 2024.

[41] J. Achiam, S. Adler, S. Agarwal, L. Ahmad, I. Akkaya, F. L. Aleman, D. Almeida, J. Altenschmidt, S. Altman, S. Anadkat *et al.*, "Gpt-4 technical report," *arXiv preprint arXiv:2303.08774*, 2023.

[42] D. Guo, D. Yang, H. Zhang, J. Song, R. Zhang, R. Xu, Q. Zhu, S. Ma, P. Wang, X. Bi *et al.*, "Deepseek-r1: Incentivizing reasoning capability in llms via reinforcement learning," *arXiv preprint arXiv:2501.12948*, 2025.

[43] M. Janiszewski, A. Felkner, P. Lewandowski, M. Rytel, and H. Romanowski, "Automatic actionable information processing and trust management towards safer internet of things," *Sensors*, vol. 21, no. 13, p. 4359, 2021.

[44] Y. Chen, J. Benton, A. Radhakrishnan, J. U. C. Denison, J. Schulman, A. Somani, P. Hase, M. W. F. R. V. Mikulik, S. Bowman, J. L. J. Kaplan *et al.*, "Reasoning models don't always say what they think." [Online]. Available: https://assets.anthropic.com/m/71876fabef0f0ed4/original/reasoning_models_paper.pdf

[45] D. Dhinakaran, S. Sankar, D. Selvaraj, and S. E. Raja, "Privacy-preserving data in iot-based cloud systems: A comprehensive survey with ai integration," *arXiv preprint arXiv:2401.00794*, 2024.

[46] T. Magara and Y. Zhou, "Internet of things (iot) of smart homes: privacy and security," *Journal of Electrical and Computer Engineering*, vol. 2024, no. 1, p. 7716956, 2024.