A SYSTEMATIC LITERATURE REVIEW: CONSUMER PERCEPTIONS OF AI-DRIVEN SECURITY AND PRIVACY LABELING FOR IOT DEVICES

By

LAWREY L. FRANCIS

B.S., University of The West Indies Mona Campus, 1989

M.S., New Jersey Institute of Technology, 1994

M.B.A., New Jersey Institute of Technology, 2003

M.S., Georgia State University, 2019

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment of the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2026

Consumer perceptions of AI-driven security and privacy labeling for IoT devices

Lawrey Francis, *Middle Georgia State University, lawrey.francis@mga.edu*

Abstract

The Internet of Things (IoT) has expanded the capabilities of the internet, establishing connectivity that impacts all aspects of our lives. AI enhances the cybersecurity landscape by addressing threats, data breaches, and risks, improving usability and user experience through dynamic security responses, and increasing efficiency. However, the promise of continued acceptance and positive perception with extensive implementation remains elusive. Numerous data breaches, device complexity, IoT security, and questionable data privacy practices adversely affect users' perceptions of IoT devices. This systematic Literature Review examines consumers' perceptions due to the lack of technical expertise to assess the security and privacy implications of IoT devices. This study highlights the capability of AI-driven labeling systems to bridge the gap between perception and device risk by providing clear, accessible summaries of collected data, its use, and the specific security safeguards required. The study aims to raise awareness of IoT security issues and suggest improvements for user understanding and safety.

***Keywords*:** artificial intelligence (AI), Internet of Things (IoT) security, data privacy, user perception.

Introduction

The Internet of Things (IoT) refers to internet-connected physical devices that collect, transmit, and act on data through embedded sensors and software. The capability of seamless connectivity to IoT devices enables attackers to access them anytime, anywhere (Sadhu et al., 2022). Consumers are constantly reminded of the security and privacy risks posed by each reported data breach, underscoring the need to raise awareness of IoT security issues. The increased use of IoT devices, as we embrace new Smart technologies, has raised significant concerns about privacy, security, and user trust (Sadhu et al., 2022). With resource constraints limiting the use of robust security, IoT devices maintain persistent connections, acting as expanded attack surfaces. This systematic Literature Review examines consumers' perceptions due to the lack of technical expertise to assess the security and privacy implications of IoT devices (Sadhu et al., 2022). Although information is available on websites and static labels, the study explores the need for greater transparency to help users understand device capabilities, security posture, vulnerabilities, and risks (Malhotra et al., 2021; Sadhu et al., 2022). This research will highlight the capability for AI-driven labeling systems to bridge this gap by providing clear, accessible summaries of what data a device collects, how it is used, and the specific security safeguards required. The study aims to raise awareness of IoT security issues and suggest improvements for user understanding and safety.

The problem addressed in this study is the absence of a standardized, user-focused AI-driven labeling framework for IoT security and privacy, which impacts consumer perceptions of trust and informed decision-making. As everyday activities incorporate more Internet of Things (IoT) devices, the complexity and magnitude of potential security risks have increased. Most consumers need more technical expertise to assess the security and privacy implications of these devices, exposing them to vulnerabilities and threats (Malhotra et al., 2021; Sadhu et al., 2022). The lack of awareness can result in increased exposure to compromised credentials, to attacker surveillance via insecure cameras, and to hijacking phones, computers, and appliances connected to a wireless network.

This study proposes and examines the impact of AI-generated, color-coded IoT security labels on consumer perceptions. A qualitative systematic literature review is utilized to explore how Artificial Intelligence (AI)

can foster user-centric awareness of IoT devices. The review examines current research on AI-generated security labels and users' perceptions of security, privacy, and data practices related to connected devices and personal information. Insights gained will inform the design of innovative, AI-driven interventions to address vulnerabilities in the consumer IoT environment, with potential implications for improving security practices and user trust. This research will answer the following questions:

RQ: What are the emerging themes on the perceptions of the impact of AI-driven, user-centric security and privacy labeling systems for IoT devices?

Review of Literature

The literature review examines emerging privacy concerns, user trust, and IoT security issues. It explores the potential to leverage AI to address these challenges, the development of AI-driven labeling systems as a possible solution, and their impact on consumer perceptions.

Security and privacy challenges in IoT

The rapid growth of IoT devices raises significant privacy and security concerns, with billions now in use (Al-Shateri et al., 2024). Vulnerabilities from wireless sensor networks (WSNs) and RFID technology are expanding cybersecurity risks (Malhotra et al., 2021). Alotaibi (2023) highlighted the need for robust security frameworks in Industrial IoT, identifying common attack vectors like data breaches and unauthorized access. Zhukabayeva et al. (2024) examine IIoT cybersecurity challenges and future research directions. Mendez Mena et al. (2018) discuss IoT security architecture, where persistent issues include a lack of standardized protocols and high resource demands (Sadhu et al., 2022; Seiger et al., 2021).
The importance of AI-driven systems for automating security tasks and enhancing incident response is increasingly recognized. Malhotra et al. (2021) emphasize the potential impact of their research, highlighting the need for continuous monitoring and intelligent intrusion detection systems (IDS) to safeguard the expanding Internet of Things (IoT) environment. These themes are not just significant but crucial in the face of the growing cybersecurity threat. IoT capabilities can precipitate threats such as data interception and device spoofing, supporting the need for transparency in security protocols (Zhou et al., 2019). The authors also emphasized the need for new solutions to counter the unique security threats posed by the ever-expanding IoT device landscape.

Sadhu et al. (2022) identify several key security threats to the Internet of Things (IoT), including Distributed Denial-of-Service (DDoS) attacks, unauthorized access, and data breaches. To address these threats, they propose blockchain and cryptographic measures as potential solutions. Ongoing challenges, such as the absence of standardized security protocols and the high resource demands of current frameworks (Seiger et al., 2021; Sadhu et al., 2022), are security and privacy concerns for IoT devices. The growing role of AI-driven systems, which automate routine security tasks and identify emerging threats, enables faster, more effective incident response and more efficient mitigation strategies.

AI driven labeling and machine learning's (ML) role in enhancing IoT security

AI-driven labeling systems address IoT security and privacy challenges by providing users with clear, real-time information about device security status (Ishibashi et al., 2022). The labels summarize key security features and risks, making it easier for users to manage risks (Ma et al., 2024). AI systems can adapt to real-time changes in device behavior, ensuring information remains accurate in the dynamic IoT environment (Zhou et al., 2019). Jouini et al. (2024) proposed a machine learning methodology for IoT label that classifies device and traffic risk levels and impacts consumer perceptions. Furthermore, Ishibashi et al. (2022) reviewed supervised and unsupervised deep learning approaches for anomaly

detection in network intrusion detection systems (NIDS) and attack classification, which could enhance dataset processing, security labeling, and alerting.

Further refinement of AI-driven device labeling relies on robust feature selection that balances efficiency and accuracy. For example, Keserwani et al. (2023) and Nazir et al. (2023) focus on feature selection and optimization for labeling in intrusion detection systems (IDSs). This supports the development of efficient AI-driven labeling models suitable for resource-constrained IoT devices. Similarly, Selem et al. (2024) demonstrate the potential of deep learning (DL) for labeling IoT network traffic as normal or abnormal. This is directly applicable to labeling device behavior. Exploring the use of AI for labeling vulnerabilities suggests that such techniques could label devices based on identified weaknesses (Ma et al., 2024). The analysis reveals an approach that shifts from a focus on optimization (Keserwani et al., 2023; Nazir et al., 2023) to learning (Selem et al., 2024) and automation (Ma et al., 2024), advancing efficient, scalable labeling. Gaps in handling zero-day vulnerabilities, a lack of generative learning, and an inability to detect and address adversarial situations that could evade detection were noted.

Alharbi et al. (2024) explored the application of AI in IoT security frameworks, emphasizing the importance of transparency in fostering user trust (Bobotek & Finch, 2024; Bye et al., 2025). Their research indicated that users are more likely to trust and adopt IoT technologies when provided with clear, understandable information about the security and privacy implications of their devices. In contrast, Ishibashi et al. (2022) outlined the ongoing research in implementing AI-powered Network Intrusion Detection Systems (NIDS). By leveraging AI capabilities, datasets are used to develop, train, and fine-tune label generation to generate alerts that identify threats in network patterns. This approach involves developing an integrated virtual NIDS by training AI-powered NIDS, an ongoing project aimed at enhancing the effectiveness of threat detection and mitigation. However, there remains a gap between user experience and technical security solutions for IoT devices. To address this, Ishibashi et al. (2022) advocated generating labeled training datasets to overcome challenges in AI-powered NIDS, while Alharbi et al. (2024) emphasized transparency to foster user trust. Despite these efforts, there is a lack of standardized frameworks to measure and quantify transparency, such as explainable AI metrics, including fidelity, stability, and user comprehension scores. As a result, trust quantification remains conceptual, with limited validation of how transparency techniques, such as XAI visualization, lead to measurable adoption in consumer IoT.

Leveraging the use of AI-driven labels into the IoT frameworks

The integration of AI-driven labels into the IoT framework is not just about security but also about creating a more user-friendly experience. Radanliev et al. (2021) noted that a user-centric design, with a simplified interface and clear, actionable security information, can significantly enhance user engagement, trust, and perceptions in IoT technologies. Focusing on user-friendliness reassures users about the ease of use of IoT technologies. To explore the similarities and differences among the authors, a unified Cybersecurity Framework (Khan et al., 2025) can use an extensible architecture that addresses security, privacy, and operational efficiency while fostering compliance with applicable regulations.

Methodology

Building on the identified research gaps, the study employs a systematic literature review following the PRISMA framework to ensure rigor and transparency in the evaluation of the literature (Page et al., 2021). The sections below outline the methodology used to identify, screen, and analyze relevant studies, following a structured synthesis of AI use in users' perceptions of IoT security and privacy.

Research design

This research employs a systematic literature review to evaluate the impact of AI on IoT device security from a user-centered perspective. A systematic review permits a structured analysis of existing research and yields comprehensive, reliable themes (Creswell et al., 2018). This study evaluates the effect of AI on securing IoT devices and assesses the impact of AI-generated labels on users' perceptions of privacy and security.

Systematic review approach

The research adheres to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to promote transparency and rigor in the selection and analysis of the literature. PRISMA includes four phases: identification, screening, eligibility, and inclusion, as outlined by Page et al. (2021). A thematic analysis was performed to link themes to the key research questions. The thematic coding software NVivo assisted in classifying themes and patterns identified in the literature. This analysis enables identification of codes, mapping of themes, and ongoing refinements to enhance rigor, replicability, and confidence in the results.

Eligibility criteria and study selection

A set of predefined inclusion and exclusion criteria enabled the selection of studies, ensuring a focused and relevant review (see Table 1). These criteria narrow the scope of the research by excluding studies unrelated to AI, IoT security, and user perception. Studies were selected if they were peer-reviewed and provided empirical or theoretical insight into transparency, explainability, privacy, or risk, relevant to consumer perception or understanding.

Table 1

Inclusion and exclusion criteria

Criteria	Inclusion	Exclusion
Publication Type	Peer-reviewed studies published between 2018 and 2025	Editorials, abstracts, and non-peer-reviewed
Language	English-language publications	Non English-language
Focus Area	Studies focusing on AI in IoT Security, IoT devices, AI models, ML, DL, AI-driven labels, AI-enabled and AI User-centric solutions	Studies unrelated
Content	Articles addressing AI, IoT, Cybersecurity, and user perception, user experience	Irrelevant topics outside AI enabled solutions and IoT security

Search strategy

The Boolean searches below were performed across all databases in the library discovery portal:

- "Artificial Intelligence" OR "AI" OR "AI-Enable" OR "AI-Driven"
- "Internet of Things" OR "IoT"
- "Security" OR "privacy" OR "perception"
- "AI Model" OR "Machine Learning" OR "ML" OR "Deep Learning" OR "DL"

- “label” OR “labels” OR “labeling” OR “Color-coded”
- “user-centric” OR “user experience” OR "user-focus"

Searches were restricted to peer-reviewed publications in English published between 2018 and 2025.

Databases:

- Galileo
- Google Scholar
- IEEE Xplore
- ScienceDirect
- Semantic Scholar

Data extraction and thematic synthesis

Search results filtering was critical for identifying relevant insights and promoting consistent thematic categorization (see Figure 1). Analysis was performed after extracting search data, filtering with Zotero, and using NVivo to distill related information into thematic categories, with a focus on the use of AI-generated labels to secure IoT devices and protect data privacy. The filtering performed with Zotero excluded articles that did not include a combination of IoT, AI, perception, user-centric, or human-centric in the abstract. The approach extracts keywords, phrases, and code text sections to generate themes such as IoT security, AI-enabled labels, user-centric, user-focused, user’s perception, AI-generated color-coded labels, data security, and privacy. The data extracted included:

- Author(s), publication year
- Focus area (IoT security, AI-enabled labels, user-centric, user-focus, user’s perception, AI-generated color-coded labels, data security, and privacy)
- Main themes and implications

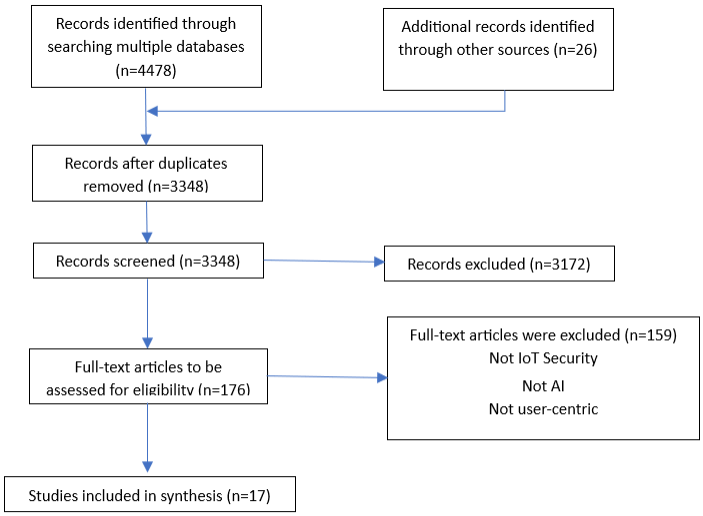

Figure 1. PRISMA 2020 flow diagram template for systematic reviews (Page et al., 2021).

NVivo was vital for identifying patterns, organizing data, and generating insights across studies. The analysis focused on the following primary themes:

- Security challenges to IoT devices
- AI impact on device security
- Factors affecting users’ perception of IoT security and data privacy

- The effectiveness of AI-enabled tools on users' perception, and understanding of user-centric solutions

This method employed a systematic approach to identify trends, similarities, and differences when comparing the selected studies from the initial search.

Risk of Bias

Study selection and thematic coding were performed by a single reviewer. To minimize bias, coding decisions were predefined and aligned with the research questions. Iterative refinement was performed using NVivo for qualitative coding and comparison across studies. Utilizing PRISMA ensured proper systematic review structure, a comprehensive literature review, promoted rigor, and addressed reporting bias. This approach promotes rigor and transparency in evaluating the impact of AI-enabled labeling in IoT security and privacy. Utilizing this approach will ensure the validity and reliability of the themes, distilling the insights into the capabilities and transformative potential of AI in the IoT landscape.

Results

The PRISMA-informed screening process identified 17 studies on AI-enabled, user-centric security and data privacy labels for IoT devices. Although none of the studies focused exclusively on "AI-enabled labels", all made worthwhile contributions to one or more parts of the AI, Labeling Mechanism, Trust, and Understanding framework. The following table presents a thematic analysis of the themes, organized by relevant themes from the review (see Table 2).

Table 2

Results

	Theme	Key Themes	Sources
1	Security challenges to IoT devices	Security and privacy challenges in IoT require user-friendly communication of risks and protections	Zhou et al, Demertzi et al, Ndaguba et al, Balaji et al, Zhukabayeva et al, Silva et al
2	AI impact on device security	Privacy-aware design with clear labeling improves user acceptance in smart home and applications	Elkhodr et al, Kaur et al, El-Gendy et al, Grgurić et al, Jouini et al
3	Factors affecting users' perception of IoT security and data privacy	User-centric security artifacts increase trust	Lola et al, Ystgaard et al, Ishibashi et al
4	The effectiveness of AI-enabled tools on users' perception, and understanding of user-centric solutions	Trust and clarity are key system requirements, Privacy awareness improves user confidence	Ndaguba et al, Nunes et al, Allen et al, Gholamhosseini et al, Deshmukh et al

Impact of AI-Driven user-centric labels

Transparency as a Perception Driver

The results, as they relate to the research question, showed that consumers viewed AI-enabled, user-centric labels positively when such systems promote visibility and clearly understandable information about IoT device security, and when they enhance perceived user control. Lola et al. (2023) demonstrate that rule-

based transparency capabilities increase user assurance and control by enabling verification of what is stated on a static label and the device's configuration. Studies examining human-centric and interpretability security mechanisms demonstrated that users' trust and security perceptions increased (Ystgaard et al. 2023). Similarly, Grgurić et al. (2019) show that privacy-aware systems in smart homes improve user acceptance by making data practices clear and more understandable to non-technical users.

Usability and Clarity

Usability and clarity were also associated with a favorable user perception. Ndaguba et al. (2023) noted that user experience in IoT environments is influenced by clear communication about security and functionality, demonstrating that "usability and clarity influence consumer trust" in a smart environment. Balaji et al. (2019) also identify "complexity and a lack of clarity" as barriers to IoT adoption. These themes suggest that AI-enabled labels must promote clarity and easily understandable information. Allen et al. (2024) denote that IoT apps with hidden vulnerabilities undermine trust when risks are not obvious. In light of this, AI-generated labels that clearly outline IoT risk posture in user-friendly formats can correct misperceptions about device capabilities and user awareness.

Legitimacy and Perceived Control

Nunes et al. (2024) show that user-centric security information enhances perceived legitimacy and promotes system acceptance. This suggests that when security posture is communicated with AI-enabled labels in clearly understandable formats, users perceive greater control over the IoT device environment. The evidence from the articles reviewed for the research question indicates users are more inclined to perceive AI-enabled, user-centric labeling systems positively. This favorable perception can be achieved by using labels that increase transparency, reduce complexity, promote legitimacy, and enhance perceived user control.

Impact of AI-Driven labels on understanding risks

Risk Translation

The studies, as they relate to the research question, indicate that "AI-driven labeling systems improve consumer understanding of IoT security and privacy risks by simplifying complex technical concepts into interpretable representations". Demertzi et al. (2023) in their work to promote clarity in a risk-level map of multiple privacy dimensions within IIoT for non-technical users. Zhou et al. (2019) also describe complex IoT threat surfaces that can be confusing to users at times. AI-enabled labels can build on this effort, serving as translation layers that simplify complex technical risk into understandable summaries or representations, such as graded risk levels, contextual alerts, or color-coded visuals.

Explainable AI as a Comprehension Bridge

Kaur et al. (2025) argue that explainable AI frameworks promote transparency in IoT decision-making, thereby improving user trust and understanding. El-Gendy et al. (2023) highlight the comprehension gap created by black-box ML systems. The combination of these themes suggests that "AI-enabled labels should include explainable features to enhance comprehension" (El-Gendy et al., 2023; Kaur et al., 2025), rather than only providing outputs.

Context-Awareness and Dynamic Understanding

Elkhodr et al. (2024) propose using AI-enabled context-aware systems to improve data security management and promote user understanding through semantic labeling. Grgurić et al emphasize that

privacy-aware design with clear labeling improves user acceptance in smart homes and healthcare applications. These research studies promote the concept of dynamic, context-aware labels rather than the current static ones. Jouini et al. (2024) also noted that ML applications at the edge require user awareness of distributed security and privacy processing, reinforcing the need for labels to fill the information gap.
The evidence from the articles reviewed for the second research question indicates that AI-enabled labels enhance users' understanding. This is accomplished by translating abstract risks into understandable summaries, utilizing explainable AI to enhance transparency, using context-aware labels to understand risk in real time, and bridging the non-technical knowledge gap.

Discussion of Themes

Given the concerns and challenges posed by the proliferation of IoT devices and the enormous capabilities of AI, this discussion examines the importance of themes on user trust, perceptions, and understanding. The themes of this research outline the continued threats and vulnerabilities associated with the increased adoption of IoT devices, as well as the potential and capabilities AI demonstrates to shape users' perceptions. Although advanced security controls are increasingly included within IoT systems, users often lack visibility into how these controls function or how they protect personal data (Demertzi et al., 2023; Zhou et al., 2019). Taken together, the literature suggests that this lack of visibility plays a central role in shaping user perceptions. Instead of looking at security based on technical strength, users form perceptions based on their ability to understand device behavior, data practices, and associated risks.

A major insight from this review is that consumer trust in IoT systems is influenced by how security and privacy are represented. The studies point to a gap between abstract privacy dimensions and users' capacity to relate them to tangible device risks. Labels can serve as representation tools to help bridge this gap by translating complex technical information into formats that users can interpret. The themes reveal that a lack of visibility plays a central role in shaping user perception and efforts to implement system-wide transparency and privacy awareness improve user confidence and perception.

The themes suggest that additional steps to create explainable ML systems can secure users' trust. Leveraging AI explanation techniques will enhance risk comprehension and support the use of labels as visual outputs. From an interpretive perspective, the role of explainable AI (XAI) extends beyond model transparency to include positive user responses to rule-based, transparent security controls and to improve understanding of security and privacy trade-offs (Lola et al., 2023; Ndaguba et al., 2023), thereby promoting trust in IoT devices' security features. The impact of user-centric, transparent design on user experience (UX) also increases trust and adoption, strengthening the case for explainable AI outputs in labels (Kaur et al., 2025).

Promoting a human-centric approach consistent with user-centric IoT design can improve trust and perceptions when IoT device security is presented in human-readable formats (Ystgaard et al., 2023). The studies highlight the impact of design principles that support AI-enabled label interpretability on users' understanding of IoT device security and privacy. Studies examining IoT companion applications revealed that the absence of visible indicators can expose users to undisclosed risks and limit their ability to make informed decisions (Allen et al., 2024). These themes suggest that clarity and interpretability are key foundational elements of effective security communication.

Complexity also emerges as a barrier to trust and adoption. Previous research identifies lack of trust and negative perceptions as obstacles to IoT adoption, particularly when technologies appear difficult to understand or control (Balaji et al., 2019). Analyzing the themes of this review suggests that simplified labeling does not reduce the seriousness of security concerns; instead, it promotes understanding, allowing users to play a role in improving the security and privacy of their IoT devices

Implications of themes

The research themes have several implications for the continued growth and acceptance of IoT devices, for privacy and security perceptions, and for future research engagements. The themes show that transparency affects user perception, and users respond positively to visual representations and rule-based security (Lola et al., 2023). This implies that AI-driven labels increase users' perception of control. Ystgaard et al. (2023) demonstrate that human-centric representations promote trust, showing positive implications for human-readable labels. Another implication was the impact of user-friendly visual labels on perception (Ndaguba et al., 2023) and the influence of clarity in user experience (UX) on trust and judgments. With the increased threat landscape for IoT devices, the themes align with privacy awareness (Grgurić et al., 2019) and risk visibility (Allen et al., 2024), as well as AI-driven labels that enhance users' perception and understanding of IoT device security and privacy. This study differs from prior research by exploring the use of AI-driven labeling to generate tools that empower users with a better understanding to reduce the attack surface, rather than focusing solely on new remediation, while keeping the door wide open to existing and new threats.

This research proposes utilizing an AI, Labeling Mechanism, Trust, and Understanding framework. This approach sets the stage for future research in leveraging AI to formulate more tools addressing users' behavior, such as perception, trust, and understanding, to inform decisions on IoT device selection and implementation choices. This approach will reduce cost and build confidence by allowing users to create a more secure IoT environment, starting with initial selections from AI-driven color-coded labels denoting risk level. Dynamic AI-generated labels for the security threat landscape, as IoT companion applications, would further equip users with the knowledge to participate in maintaining and enhancing their security posture, enabling decisions based on continuous monitoring with AI-enabled tools.

Conclusion

The increased number of devices has broadened the attack surface and opportunities for cyberattacks. The study highlights the need to expand AI-enabled security for IoT devices to address privacy and data security concerns. In an attempt to formulate solutions using emerging technologies, Jouini et al. (2024) and Zhou et al. (2019) undertook studies that integrated machine learning (ML) and deep learning (DL) for intrusion detection and risk assessment, reflecting a shift toward proactive security measures.

While AI-enabled labeling is mentioned in risk assessment models, there is a lack of clearly defined frameworks for user-centric transparency, and it represents a crucial, underexplored area. The literature highlights the critical need for innovative solutions to the security and privacy challenges posed by the rapid proliferation of IoT devices. AI-driven labeling systems, with their potential to enhance transparency, improve user trust, and provide real-time, adaptable security information, are promising approaches to addressing these challenges. By bridging the gap between complex technical concepts and user understanding, these solutions can significantly improve the safety and transparency of IoT environments.

References

Alharbi, S. H., Alzahrani, A. M., Syed, T. A., & Alqahtany, S. S. (2024). Integrity and privacy assurance framework for remote healthcare monitoring based on IoT. *Computers, 13*(7), 164. https://doi.org/10.3390/computers13070164

Allen, A., Mylonas, A., Vidalis, S., & Gritzalis, D. (2024). Security evaluation of companion Android applications in IoT: The case of smart security devices. *Sensors*, *24*(17), 5465. https://doi.org/10.3390/s24175465

Alotaibi, B. (2023). A survey on industrial internet of things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors*, *23*(17), 7470. https://doi.org/10.3390/s23177470

Al-Shateri, A. A. H., Rashid, R. A., Aburaya, A., & Muhammad, N. A. (2024). Luna: A benchmark project in the convergence of artificial intelligence and Internet of Things for home automation. *2024 IEEE International Conference on Advanced Telecommunication and Networking Technologies (ATNT)* (pp. 1–4). *IEEE*. https://doi.org/10.1109/ATNT61688.2024.10719226

Balaji, S., Nathani, K., & Santhakumar, R. (2019). IoT technology, applications and challenges: A contemporary survey. *Wireless Personal Communications,108*(1), 363–388. https://doi.org/10.1007/s11277-019-06407-w

Bobotek, J. P., & Finch, B. E. (2024). Balancing cybersecurity threats in smart cities: Is the potential convenience of "smart" intersections worth the risk? *Computer & Internet Lawyer, 41*(9), 6–7.

Bye, A., Wilson-Lemoine, E., Trevillion, K., Carter, B., & Dutta, R. (2025). Factors that affect clinical youth engagement in digital mental health research: a qualitative sub-study nested within a prospective cohort study. *BMC Medical Research Methodology*, *25*(1), 1–15. https://doi.org/10.1186/s12874-025-02571-9

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design.* (Fourth edition.). SAGE Publications.

Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An overview of privacy dimensions on the Industrial Internet of Things (IIoT). *Algorithms*, *16(8)*, 378. https://doi.org/10.3390/a16080378

Deshmukh, A., de la Rosa, P. E., Rodriguez, R. V., & Dasari, S. (2025). Enhancing Privacy in IoT-enabled digital infrastructure: Evaluating federated learning for intrusion and fraud detection. *Sensors, 25*(10), 3043. https://doi.org/10.3390/s25103043

El-Gendy, S., Elsayed, M. S., Anca Jurcut, A., Azer, M., A. (2023). Privacy preservation using machine learning in the Internet of Things. *Mathematics, 11*(16), 3477. https://doi.org/10.3390/math11163477

Elkhodr, M., Khan, S., & Gide, E. (2024). A novel semantic IoT middleware for secure data management: Blockchain and AI-driven context awareness. *Future Internet, 16*(1), 22. https://doi.org/10.3390/fi16010022

Gholamhosseini, L., Sadoughi, F., Rezayi, S., & Nasiri, S. (2024). Identifying cloud internet of things requirements in healthcare: A Delphi-based study. *Journal of Supercomputing, 80*(14), 20201–20228. https://doi.org/10.1007/s11227-024-06253-z

Grgurić, A., Mošmondor, M., Huljenić. D. (2019). The SmartHabits: An intelligent privacy-aware home care assistance system. *Sensors, 19*(4), 907. https://doi.org/10.3390/s19040907

Ishibashi, R., Miyamoto, K., Han, C., Ban, T., Takahashi, T., Takeuchi, J. (2022). Generating labeled training datasets towards unified network intrusion detection systems. *IEEE Access, 10*, 2022. https://doi.org/10.1109/ACCESS.2022.3176098

Jouini, O., Sethom, K., Namoun, A., Aljohani, N., Alanazi, M. H., & Alanazi, M. N. (2024). A survey of machine learning in edge computing: Techniques, frameworks, applications, issues, and research directions. *Technologies, 12*(6), 81. https://doi.org/10.3390/technologies12060081

Keserwani, P. K., Govil, M. C., & Pilli, E. S. (2023). An effective NIDS framework based on a comprehensive survey of feature optimization and classification techniques. *Neural Computing & Applications, 35*(7), 4993–5013. https://doi.org/10.1007/s00521-021-06093-5

Khan, H. U., Khan, R. A., Alwageed, H. S., Almagrabi, A. O., Ayouni, S., & Maddeh, M. (2025). AI-driven cybersecurity framework for software development based on the ANN-ISM paradigm. *Scientific Reports, 15(1)*, 1–45. https://doi.org/10.1038/s41598-025-97204-y

Kaur, N., Gupta, L. (2025). Securing the 6G–IoT Environment: A Framework for enhancing transparency in artificial intelligence decision-making through explainable artificial intelligence. *Sensors, 25*(3), 854. https://doi.org/10.3390/s25030854

Lola, J., Serrão, C., & Casal, J. (2023). Towards Transparent and Secure IoT: Improving the security and privacy through a user-centric rules-based system. *Electronics, 12*(12), 2589. https://doi.org/10.3390/electronics12122589

Ma, P., Zhu, L., & Zhang, C. (2024). Research on vulnerability mining method based on artificial intelligence in Internet of Things. *2024 IEEE 2nd International Conference on Image Processing and Computer Applications (ICIPCA)* (pp. 1470–1473). IEEE. https://doi.org/10.1109/ICIPCA61593.2024.10709035

Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., Hong, W.-C., & Calafate, C. T. (2021). Internet of Things: Evolution, concerns and security challenges. *Sensors, 21*(5), 1809. https://doi.org/10.3390/s21051809

Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective*, *27*(3), 162–182. https://doi.org/10.1080/19393555.2018.1458258

Ndaguba, E., Cilliers, J., Ghosh, S., Herath, S., & Mussi, E. T. (2023). Operability of smart spaces in urban environments: A systematic review on enhancing functionality and user experience. *Sensors, 23*(15), 6938. https://doi.org/10.3390/s23156938

Nunes, M., Kayan, H., Burnap, P., Perera, C., Dykes, J. (2024). Exploiting user-centred design to secure industrial control systems. *Frontiers in the Internet of Things, 3*. https://doi.org/10.3389/friot.2024.1436023

Radanliev, P., De Roure, D., Ani, U., & Carvalho, G. (2021). The ethics of shared COVID-19 risks: An epistemological framework for ethical health technology assessment of risk in vaccine supply chain infrastructures. *Health and Technology, 11*(5), 1083–1091. https://doi.org/10.1007/s12553-021-00565-3

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Journal of Clinical Epidemiology, 134*, 178–189. https://doi.org/10.1016/j.jclinepi.2021.03.001

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and solutions survey. *Sensors, 22*(19), 7433. https://doi.org/10.3390/s22197433

Seiger, R., Kühn, R., Korzetz, M., & Abmann, U. (2021). HoloFlows: Modeling of processes for the Internet of Things in mixed reality. *Software & Systems Modeling, 20*(5), 1465–1489. https://doi.org/10.1007/s10270-020-00859-6

Selem, M., Farah, J., & Korbaa, O. (2024). Deep learning for intrusion detection in IoT networks. *Research Square (Research Square)*. https://doi.org/10.21203/rs.3.rs-4306367/v1

Silva, A. L. M., Pérez, A. J. de J., & Kofuji, S. T. (2019). Interoperability in semantic Web of Things: Design issues and solutions. *International Journal of Communication Systems, 32(6)*, N.PAG. https://doi.org/10.1002/dac.3911

Ystgaard, K. F., Atzori, L., Palma, D., Heegaard, P. E., Bertheussen, L. E., Jensen, M. R., & De Moor, K. (2023). Review of the theory, principles, and design requirements of human-centric Internet of Things (IoT). *Journal of Ambient Intelligence & Humanized Computing, 14(3)*, 2827–2859. https://doi.org/10.1007/s12652-023-04539-3

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The Effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *Internet of Things Journal, IEEE, IEEE Internet Things J, 6*(2), 1606–1616. https://doi.org/10.1109/JIOT.2018.2847733

Zhukabayeva, T., Zholshiyeva, L., & Karabayev, N. (2024). Future directions of cybersecurity in industrial Internet of Things through edge computing. *2024 9th International Conference on Computer Science and Engineering (UBMK)*, (pp. 1-6). https://doi.org/10.1109/UBMK63289.2024.10773586