Journal of Edge Computing, **2024**, 3(2), pp. 207-223 https://doi.org/10.55056/jec.747

The sweet taste of IoT deception: an adaptive honeypot framework for design and evaluation

Dmytro S. Morozov[1], *Andrii A.* Yefimenko[1], *Tetiana M.* Nikitchuk[1], *Roman O.* Kolomiiets[1] and *Serhiy O.* Semerikov[2,3,1,4,5]

[1]*Zhytomyr Polytechnic State University, 103 Chudnivsyka Str., Zhytomyr, 10005, Ukraine*
[2]*Kryvyi Rih State Pedagogical University, 54 Universytetskyi Ave., Kryvyi Rih, 50086, Ukraine*
[3]*Institute for Digitalisation of Education of the NAES of Ukraine, 9 M. Berlynskoho Str., Kyiv, 04060, Ukraine*
[4]*Kryvyi Rih National University, 11 Vitalii Matusevych Str., Kryvyi Rih, 50027, Ukraine*
[5]*Academy of Cognitive and Natural Sciences, Ukrainian Branch, 54 Gagarin Ave., Kryvyi Rih, 50086, Ukraine*

Abstract. The rapid proliferation of Internet of Things (IoT) devices has introduced unprecedented security challenges for critical infrastructure systems. Honeypots and honeynets have emerged as promising deception technologies for detecting, deflecting, and investigating IoT-specific threats. In this paper, we propose an integrated framework for the design, implementation, and evaluation of adaptive honeypots in IoT environments. The framework consists of two key components: (1) an adaptive honeypot architecture that dynamically adjusts its behaviour based on observed attack patterns and (2) an evaluation methodology with quantitative metrics to assess the effectiveness of IoT honeypots. We discuss the current usage and future potential of this integrated framework in the context of critical infrastructure protection, highlighting challenges and opportunities for collaborative defence against evolving cyber threats.[1]

Keywords: adaptive honeypots, IoT security, deception technology, machine learning, intrusion detection, evaluation metrics, critical infrastructure protection, cyber threat intelligence, software-defined networking, collaborative defence

1. Introduction

The rapid proliferation of Internet of Things (IoT) devices has introduced unprecedented convenience and efficiency across various domains. However, this growth has also ushered in a wave of cyber attacks targeting these often vulnerable systems [2]. Critical infrastructure, increasingly reliant on interconnected sensors and IoT devices, is particularly susceptible to such attacks due to the expanded attack surface [16]. A security breach in these systems can compromise sensitive data, disrupt essential services, and inflict severe economic losses [17].

[1]This paper is the further development of our work [23] presented at the 3rd Edge Computing Workshop.

morozovds@ztu.edu.ua (D. S. Morozov); yefimenko.andrii@gmail.com (A. A. Yefimenko); tnikitchuk@ukr.net (T. M. Nikitchuk); krt_kro@ztu.edu.ua (R. O. Kolomiiets); semerikov@acnsci.org (S. O. Semerikov)
https://ztu.edu.ua/teacher/138.html (D. S. Morozov); https://ztu.edu.ua/teacher/319.html (A. A. Yefimenko); https://ztu.edu.ua/teacher/132.html (T. M. Nikitchuk); https://ztu.edu.ua/teacher/125.html (R. O. Kolomiiets); https://acnsci.org/semerikov (S. O. Semerikov)
0000-0002-0807-590X (D. S. Morozov); 0000-0003-2128-4797 (A. A. Yefimenko); 0000-0002-9068-931X (T. M. Nikitchuk); 0000-0002-9020-938X (R. O. Kolomiiets); 0000-0003-0789-0272 (S. O. Semerikov)

Traditional security measures struggle to keep pace with the evolving sophistication and scale of IoT-focused cyber attacks [39]. The heterogeneity of IoT devices, coupled with their resource constraints and the variety of communication protocols they employ, further complicate the development of robust defence mechanisms [20]. Consequently, there is a pressing need for innovative detection and analysis techniques that can effectively identify and mitigate threats in IoT ecosystems [12].

Honeypots and honeynets have emerged as promising deception technologies for detecting, deflecting, and investigating IoT-specific threats. By creating decoy systems that mimic real IoT devices, honeypots can attract and capture attack traffic, providing valuable insights into attacker behaviour and tactics [26]. However, the efficacy of honeypots in the IoT domain is heavily dependent on their ability to closely emulate the characteristics and vulnerabilities of real devices while adapting to the evolving threat landscape [35].

The goal of this paper is to propose an integrated framework for adaptive honeypots in IoT environments that addresses the challenges of scalability, fidelity, and intelligence generation. We aim to answer the following research questions:

1. How can we design an adaptive honeypot architecture that dynamically adjusts its behaviour based on observed attack patterns and enables intelligence-driven deception?
2. What metrics and evaluation methodology can be used to assess the effectiveness of IoT honeypots in terms of attack interaction, intelligence gathering, and threat containment?
3. What are the current challenges and future research directions for adaptive honeypots in IoT security?

To address these questions, we propose an integrated framework that consists of two closely related components: (1) an adaptive honeypot architecture that leverages machine learning techniques to adjust its behaviour based on observed attack patterns dynamically, and (2) an evaluation framework with quantitative metrics to assess the effectiveness of IoT honeypots.

The remainder of this paper is organized as follows. Section 2 provides an overview of related work on honeypots and their applications in IoT security. Section 3.1 presents the proposed adaptive IoT honeypot framework, including its architecture, implementation, and integration with intrusion detection systems. Section 3.2 introduces the evaluation framework and metrics for assessing IoT honeypot effectiveness, along with a case study illustrating its application. Section 4 discusses the current challenges, future research directions, and potential applications of adaptive honeypots in critical infrastructure protection. Finally, section 5 concludes the paper and highlights the main contributions and future work.

2. Background and related work

Honeypots and honeynets have emerged as valuable tools for studying the behaviour of cyber attackers by luring them into isolated, monitored environments [34]. A *honeypot* is a single system designed to attract and contain attackers, while a honeynet is a network of multiple honeypots. These deceptive systems allow defenders to observe attack tactics, techniques and procedures (TTPs) without putting production systems at risk.

Honeypots are typically classified as low-interaction or high-interaction based on the level of activity an attacker is permitted to perform [22]. Low-interaction honeypots, such as Honeyd

[29], provide limited emulated services and capture limited information. High-interaction honeypots, like Sebek [4], give attackers access to real operating systems and capture detailed data but risk being used to attack other systems if not properly contained.

In the context of IoT security, honeypots have been proposed to mitigate the unique challenges of IoT devices, such as their heterogeneity, resource constraints, and use of non-standard protocols [26]. Dowling, Schukat and Melvin [9] designed an IoT honeynet architecture using a hybrid of physical devices and virtual software. Other IoT-specific honeypots emulate standard protocols like MQTT [38], CoAP [14], and UPnP [13].

For critical infrastructure security, researchers have deployed honeypots to capture threats against industrial control systems (ICS) [37]. Digital bond's SCADA honeynet includes emulated programmable logic controllers (PLCs) to analyze attacks on industrial processes [30]. Antonioli and Tippenhauer [3] proposed using MiniCPS, a toolkit for simulating cyber-physical systems, to create high-fidelity ICS honeypots.

However, existing honeypot solutions often fall short in addressing the unique challenges of IoT environments, such as the diversity of devices and protocols, resource constraints, and the need for scalable, adaptive deception [9, 26]. Many prior works focus on emulating specific IoT devices or protocols in isolation, needing a flexible framework for creating comprehensive deception environments that can evolve with the changing threat landscape [13, 38]. Additionally, limited research exists on the strategic deployment of multiple interactive honeypots to provide deceptive views of an IoT or ICS network rather than a single device.

3. Integrated framework proposal

3.1. Adaptive IoT honeypot framework

3.1.1. Architecture and implementation

Honeypots and honeynets come in various types, each with strengths and weaknesses when applied to IoT and critical infrastructure security. We classify them into three main categories:

1. *Physical honeypots* use real IoT devices, providing high interactivity and realism but limited scalability due to hardware costs [26]. They are well-suited for studying attacks that exploit device-specific vulnerabilities. For critical infrastructure, physical honeypots can incorporate fundamental ICS components like PLCs and RTUs to mimic industrial environments closely [37].
2. *Virtual honeypots* emulate IoT devices in software, enabling greater deployment flexibility and lower costs than physical honeypots. However, they may lack fidelity and struggle to emulate proprietary IoT protocols [9]. Virtual machines can simulate large networks of ICS devices for honeynet deployment [3].
3. *Hybrid honeypots* combine physical and virtual elements for balanced realism and scalability [28]. They are promising for IoT scenarios with diverse device types. In ICS, hybrid honeypots could mix real hardware for critical components with emulated secondary devices.

Table 1 compares different types of honeypots (low-, medium-, high-interaction) across various dimensions relevant to IoT environments.

Table 1
Comparison of honeypot types for IoT environments.

Type	Low-interaction	Medium-interaction	High-interaction
Emulation	Limited, static services	Partial, scripted interactions	Full OS and services
Scalability	High, low resource usage	Moderate, depends on emulation complexity	Low, resource-intensive
Fidelity	Low, easily detectable	Moderate, can mimic some IoT behaviours	High, indistinguishable from real devices
Risk	Low, attacker confined to honeypot	Moderate, some risk of compromise	High, can be used as pivot point
Maintenance	Easy, minimal configuration	Moderate, requires updating scripts	Difficult, needs constant patching and monitoring
Intelligence gathering	Limited, mainly attack signatures	Moderate, some insight into TTPs	Extensive, can reveal new exploits and strategies
IoT suitability	Low, insufficient emulation of IoT protocols and functionalities	Moderate, can mimic common IoT services but lacks device-specific behaviours	High, can closely replicate IoT devices but challenging to scale and maintain
Example	Honeyd [29], Dionaea [8]	Cowrie [25], Conpot [6]	IoTCandyJar [28], ThingPot [40]

To adapt honeypots for IoT and critical infrastructure, we propose:

- *Modularity:* honeypots should support easy swapping of emulated devices/protocols to match evolving IoT ecosystems (container and SDN technologies can aid such flexibility).
- *Deceptive interfaces:* honeypots should expose not just individual devices but deceptive network topologies and cross-device interactions to mimic real environments better and support threat analysis.
- *Safety:* to prevent honeypot compromise from impacting real systems, strict network isolation and device hardening is critical, especially for physical honeypots in ICS with potential physical consequences.
- *Specialized interaction:* honeypots should implement not just generic protocols but also IoT/ICS-specific functionality, like device pairing or control system alarming, to engage attackers and learn domain-specific TTPs.

By mixing honeypot types, addressing IoT/ICS-specific needs, and crafting realistic deceptive environments, defenders can better understand and mitigate novel threats in these domains. The HoneyScope architecture embodies these principles to enable effective IoT deception [1].

Figure 1 illustrates our proposed IoT honeynet architecture, which leverages SDN to create device-group-specific deceptive views. The key components are:

- *IoT honeynet controller* orchestrates the overall honeynet and adaptively configures the SDN gateway based on attacker behaviours.

- *SDN gateway* presents different virtual network topologies (honeypot device groups) to attackers, isolating and containing their activities.
- *Device groups* (1, 2, 3, ...) are Collections of honeypots emulating specific types of IoT devices and protocols, enabling targeted interaction and data capture.

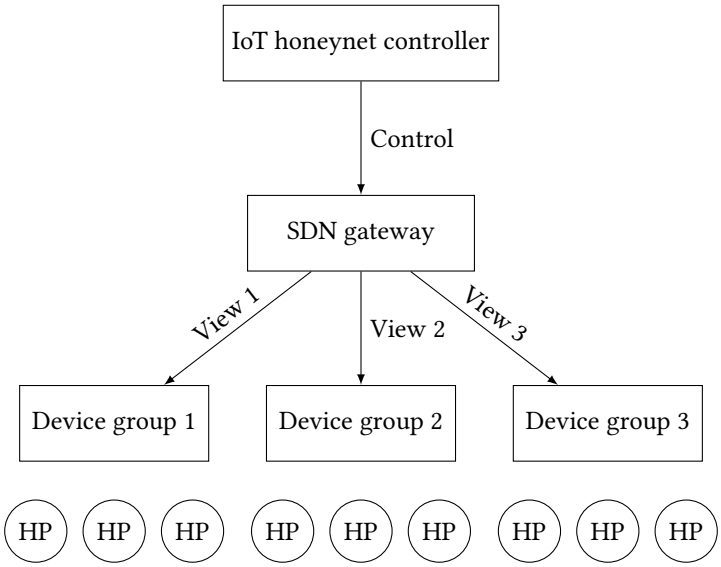


Figure 1: Proposed architecture for IoT honeynet with device-group-specific views.

The data flows from the controller to the gateway (control messages) and from the gateway to the device groups (attacker traffic redirected to appropriate honeypots). The SDN gateway, controlled by the honeynet controller, presents distinct virtual topologies to attackers based on their observed behaviours and target device groups. This architecture supports our goal of adaptive, intelligence-driven IoT deception by dynamically adjusting the honeynet based on observed attacks.

Our adaptive IoT honeypot framework is implemented using a combination of open-source tools and custom components. The key enabling technologies are:

- OpenFlow [21] is an SDN protocol used to dynamically configure the virtual network topologies and redirect traffic between honeypots and real IoT devices.
- Mininet [18] is a network emulation platform that allows the creation of realistic virtual environments, including IoT-specific protocols and services, to attract and engage attackers.
- IoTCandyJar [19] is a high-interaction honeypot used as a base for emulating detailed IoT device behaviour and vulnerabilities. We plan to extend IoTCandyJar to support a broader range of IoT protocols, such as MQTT, CoAP, and UPnP.
- Cowrie [25] is a medium-interaction SSH and Telnet honeypot used to capture attacker keystrokes and analyze their behaviour. We plan to integrate Cowrie into our framework to handle common IoT attack vectors.

- Scikit-learn [27] is a machine learning library in Python used to implement the adaptive decision-making components of the framework. We plan to train models on historical attack data to predict attacker intent and dynamically adjust the honeypot configuration [15].

The device-group-specific views are realized by leveraging the SDN controller to create virtual network segments, each containing honeypots tailored to a specific class of IoT devices (e.g., smart home appliances and industrial control systems). The controller dynamically assigns attackers to these virtual segments based on their observed behaviour and the predicted target device group. This allows for presenting a customized deception environment to each attacker while maintaining isolation and preventing lateral movement.

3.1.2. Integration with intrusion detection systems

Honeypots and honeynets are not standalone security solutions but rather components of a comprehensive defence-in-depth strategy. They are particularly effective when integrated with intrusion detection systems (IDS) to enable proactive threat discovery and informative alert generation [22].

In a typical integrated architecture, honeypots serve as decoys that attract and contain attackers while an IDS monitors their activity. The IDS can leverage the knowledge that any interaction with the honeypot is suspicious to generate high-confidence alerts with minimal false positives [29]. Conversely, the IDS can tune the honeypot's behaviour based on detected threats to optimize attacker engagement.

For IoT environments, honeypot-IDS integration offers unique challenges and opportunities:

- *Diverse data sources* IoT honeypots must feed a wide variety of IoT honeypots, providing a wide variety of device-specific log data to the IDS for analysis. This requires robust data normalization and correlation capabilities [26].
- *Edge processing* enables real-time detection on resource-constrained devices, where certain IDS functionalities may need to be offloaded to the honeypot level for local edge processing [10].
- *Adaptive deception* allows the IDS to dynamically adjust the honeypot environment, including topology, exposed vulnerabilities, and service versions, based on attacker behaviour to enhance intelligence gathering [31].
- *Cross-layer detection* in IoT addresses attack vectors across multiple layers, from physical devices to application APIs. Honeypot and IDS integration should capture and correlate events across these layers for comprehensive situational awareness [5].

HoneyScope architecture [1] exemplifies honeypot-IDS integration for IoT, using SDN to create device-group-specific deceptive views while leveraging IDS data for dynamic reconfigurations. Such architectures pave the way for more adaptive, intelligence-driven defence in IoT environments.

Figure 2 shows how our IoT honeypots integrate with intrusion detection systems to enable proactive defence. The key data flows are:

- *Alerts* are generated by honeypots on observed attack traffic and sent to the IDS for analysis.
- *Threat intelligence* is provided when the IDS correlates honeypot alerts with other network data, offering actionable insights used to reconfigure the honeypots for optimal attacker engagement adaptively.
- *Attack traffic* is redirected from real IoT devices to honeypots, allowing for contained analysis without posing a risk to production systems.

Honeypots capture attack traffic and feed alerts to the IDS for analysis. The IDS provides threat intelligence to reconfigure the honeypots adaptively. Such a bidirectional feedback loop enables proactive defence and high-confidence attack detection.

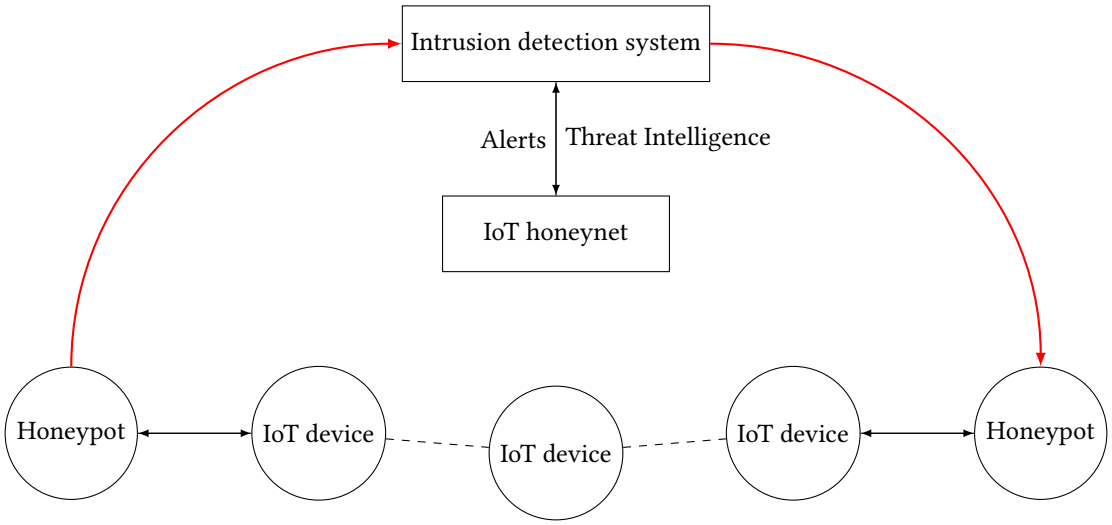


Figure 2: Integration of honeypots with IDS in an IoT network.

This integration aligns with our objective of leveraging honeypots not just for passive data collection but for active, intelligence-driven responses to IoT threats.

3.2. IoT honeypot evaluation framework

3.2.1. Evaluation metrics

Evaluating the effectiveness of honeypot and honeynet deployments in IoT environments is crucial for justifying their continued use and identifying areas for improvement. We propose the following framework and metrics for assessing IoT honeypot performance:

1. **Interaction metrics:**
    - *Attack frequency* – the number of unique attacks or suspicious interactions with the honeypot over a given time period.
    - *Attack diversity* – the variety of attack types, protocols, or IoT devices targeted, as measured by Shannon entropy or similar diversity indices [9].

- *Interaction duration* – the average time an attacker spends interacting with the honeypot, indicating the level of engagement and deception achieved [26].

2. **Intelligence metrics:**
   - *Threat intelligence volume* – the amount of actionable information collected about attacker tactics, techniques, and procedures (TTPs), such as IP addresses, malware samples, or exploited vulnerabilities [36].
   - *Intelligence novelty* – the proportion of collected intelligence that represents previously unknown threats or TTPs, as determined by comparison with existing threat databases [22].
   - *Intelligence relevance* – the degree to which collected intelligence aligns with the organization's specific IoT assets, vulnerabilities, and risk profile [1].
3. **Containment metrics:**
   - *Compromise rate* – the percentage of attacks that successfully compromise the honeypot, indicating the effectiveness of containment measures [24].
   - *Lateral movement prevention* – the ability of the honeynet to prevent attackers from pivoting to other network segments or real IoT devices, as measured by the ratio of contained to total attacks [10].

Table 2 defines the specific metrics used in our evaluation framework for assessing IoT honeypot effectiveness. These metrics were chosen to comprehensively cover the key objectives of honeypot deployment, including attacker engagement (attack frequency, diversity, duration), intelligence gathering (volume, novelty), and containment capabilities (compromise rate,

Table 2
Proposed evaluation metrics for IoT honeypots.

Metric	Description	Formula
Attack frequency	Number of unique attacks or interactions over a given time period	$\frac{\text{Number of attacks}}{\text{Time period}}$
Attack diversity	Variety of attack types, protocols, or devices targeted, measured by Shannon entropy [9]	$-\sum_{i=1}^{n} p_i \log_2 p_i$
Interaction duration	Average time an attacker spends interacting with the honeypot	$\frac{\sum_{i=1}^{n} \text{Interaction time}_i}{\text{Number of interactions}}$
Threat intelligence volume	Amount of actionable information collected about attacker TTPs	Count of unique TTPs identified
Intelligence novelty	Proportion of collected intelligence representing previously unknown threats	$\frac{\text{Number of new threats}}{\text{Total threats}}$
Intelligence relevance	Percentage of relevant intelligence items	$\frac{\text{Number of relevant intelligence items}}{\text{Total intelligence items}} \times 100\%$
Compromise rate	Percentage of attacks that successfully compromise the honeypot	$\frac{\text{Number of successful attacks}}{\text{Total attacks}} \times 100\%$
Lateral movement prevention	Ratio of contained attacks to total attacks [11]	$\frac{\text{Number of contained attacks}}{\text{Total attacks}}$

lateral movement prevention). The formulas provided enable quantitative measurement and benchmarking of honeypot performance.

The proposed evaluation metrics are tightly coupled with our adaptive IoT honeypot framework, enabling the quantitative assessment of its effectiveness in realistic deployment scenarios. For example, the interaction duration and intelligence novelty metrics directly measure the framework's ability to engage attackers and elicit novel attack techniques through its adaptive deception capabilities. Similarly, the compromise rate and lateral movement prevention metrics evaluate the effectiveness of the device-group-specific isolation and containment mechanisms.

To support the computation of these metrics, our framework includes comprehensive logging and data collection components that capture attacker interactions at various levels (network traffic, system events, honeypot logs). These raw data are processed and analyzed using the machine learning pipeline to extract relevant features and insights. The evaluation results can then be used to refine the honeypot configuration and adaptation strategies iteratively, closing the feedback loop between deployment and assessment.

3.2.2. Methodology and case studies

To illustrate the IoT honeypot evaluation framework, consider a hypothetical smart city deployment with a honeynet covering various IoT systems, such as traffic sensors, smart meters, and public Wi-Fi hotspots. Over one month, the honeynet records 100 unique attacks, targeting 12 different IoT device types (high diversity). The average interaction duration is 30 minutes, and the honeynet captures 10 unique malware samples and identifies 5 new vulnerabilities (high novelty). The compromise rate is 5% and only 1 attack successfully pivots to a real device (effective containment).

Figure 3 provides a concrete case study of applying our evaluation framework to a smart city IoT deployment. The key components are:

- *IoT device types*: the smart city includes traffic sensors, smart meters, and public Wi-Fi, each emulated by dedicated honeypots.
- *Evaluation metrics*: a range of quantitative metrics (attack frequency, diversity, duration, intelligence novelty, compromise rate, lateral movement prevention) are used to assess the honeypots' effectiveness comprehensively.
- *Data flows*: attack traffic targeting each IoT device type is captured by the corresponding honeypot for analysis and metric calculation.

Honeypots emulate different device types (traffic sensors, smart meters, public Wi-Fi) and capture attack data. The proposed metrics assess honeypot effectiveness in terms of attacker engagement, intelligence gathering, and containment capabilities.

This case study demonstrates how our evaluation framework can be applied to a real-world IoT scenario, aligning the choice of honeypots and metrics with the specific security objectives and threat landscape of smart city deployments.

Real-world evaluation faces challenges such as:

- *Ground truth* involves validating the true nature of captured threats and distinguishing real attacks from background noise or false positives [28].

- *Longitudinal analysis* requires collecting sufficient data over extended periods to identify trends and assess long-term effectiveness, which is particularly important for low-interaction honeypots [22].
- *Balancing realism and risk* focuses on configuring honeypots to be realistic enough to attract advanced attackers while minimizing the risk of compromise and potential misuse [24].

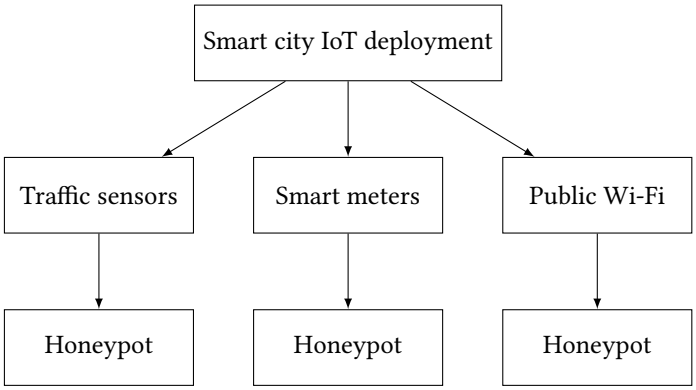
To address these challenges, organizations should use threat intelligence sharing platforms, collaborate with industry partners, and regularly update and validate their honeynet configurations based on the latest IoT threats. By combining quantitative metrics with qualitative analysis and expert judgment, this evaluation framework provides a comprehensive assessment of IoT honeypot effectiveness and helps guide future improvements.

4. Discussion

While honeypots and honeynets have shown promise for enhancing IoT security, several open issues and challenges remain to be addressed. These challenges span technical, operational, and legal domains, highlighting the need for continued research and development.

One key technical challenge is the scalability and adaptability of IoT honeypots. As the variety and complexity of IoT devices continue to grow, honeypots must be able to emulate a wide range of device types and protocols efficiently [26]. This requires modular, configurable architectures that can be easily updated to match evolving IoT ecosystems. Automated honeypot generation and configuration techniques, leveraging machine learning and network discovery tools, are a promising direction to address this challenge [9].

Another technical challenge is the fidelity of IoT honeypots. To effectively engage and deceive attackers, honeypots must closely mimic the behaviour and characteristics of real IoT devices [1]. This includes not only network protocols but also device-specific functionality, such as sensor data generation and actuation capabilities. High-interaction honeypots that incorporate real IoT hardware or advanced simulation engines are needed to provide convincing deception. However, balancing fidelity with scalability and containment remains an open problem.



Evaluation metrics:
- Attack frequency
- Attack diversity
- Interaction duration
- Threat intelligence volume
- Intelligence novelty
- Intelligence relevance
- Compromise rate
- Lateral movement prevention

Figure 3: Hypothetical case study illustrating the evaluation framework for a smart city IoT deployment.

From an operational perspective, deploying and maintaining IoT honeypots requires specialized skills and resources that may be lacking in many organizations [10]. Honeypot management platforms that simplify deployment, configuration, and data analysis tasks are needed to lower the barriers to adoption. Integration with existing security tools and workflows, such as SIEM systems and incident response playbooks, is also crucial for maximizing the value of honeypot data.

Legal and ethical challenges surrounding honeypot usage must also be carefully considered. Attracting and monitoring attacker activity raises concerns about privacy, entrapment, and liability [33]. Organizations must ensure that their honeypot deployments comply with relevant laws and regulations, such as the European Union's General Data Protection Regulation (GDPR) or the United States' Computer Fraud and Abuse Act (CFAA). Engaging with legal experts and developing clear policies for data collection, retention, and sharing can help mitigate these risks.

Figure 4 presents a research roadmap for advancing IoT honeypots, mapping key challenges to promising solution directions. The main challenges are:

- **Scalability and adaptability** – handling the growing diversity and rapid evolution of IoT devices and protocols.
- **Fidelity and realism** – closely emulating IoT-specific behaviours and vulnerabilities to engage attackers.
- **Deployment and management** – streamlining honeypot setup, configuration, and data analysis in resource-constrained environments.

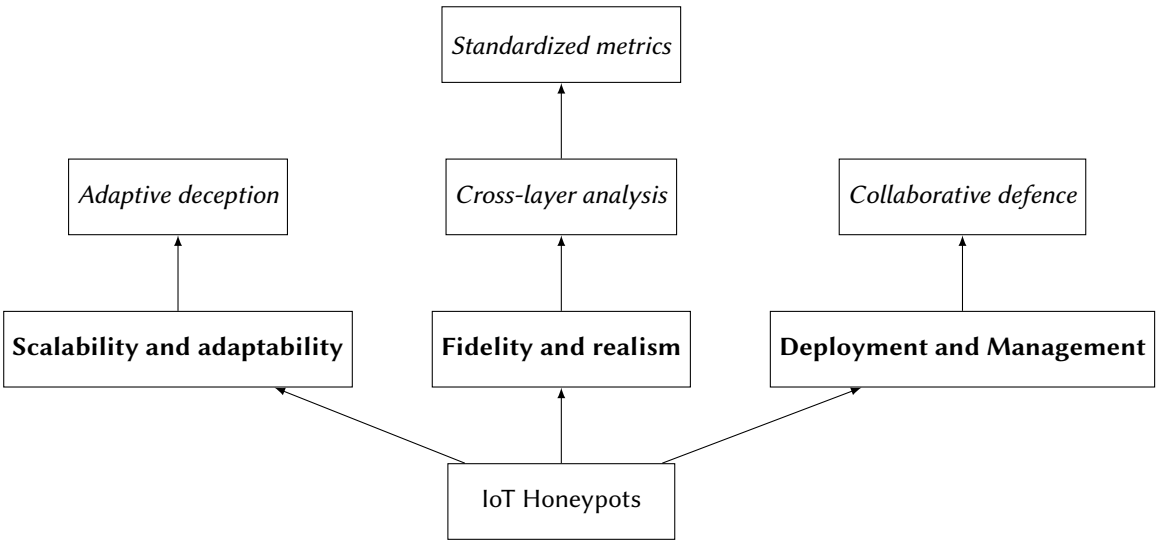


Figure 4: Research roadmap highlighting key challenges and future directions for IoT honeypots.

To address these challenges and advance the state-of-the-art in IoT honeypots, several promising research directions should be pursued:

- *Adaptive deception:* developing machine learning techniques that dynamically adjust honeypot configurations and behaviour based on attacker activity and network context [31].
- *Cross-layer analysis:* integrating network, application, and device-level data from honeypots to provide a more comprehensive view of IoT threats and attack chains [36].
- *Collaborative defence :* exploring architectures and protocols for sharing honeypot data and threat intelligence across organizations and sectors to enable collective defence against IoT threats [7].
- *Deception metrics:* defining and validating standardized metrics for evaluating the effectiveness of IoT honeypots in terms of attack attraction, intelligence gathering, and threat containment [24].

This roadmap aligns with our overall objectives by identifying the key technical and operational hurdles that must be overcome to realize honeypots' full potential in securing IoT ecosystems against evolving threats. By providing a structured agenda for future research, we aim to accelerate the development and real-world adoption of next-generation IoT honeypot solutions.

Our adaptive IoT honeypot framework, while addressing key challenges in terms of scalability, fidelity, and intelligence generation, also opens up several avenues for further research and improvement. One critical area is the development of more advanced machine-learning techniques for attacker profiling and intent prediction. Our current implementation relies on relatively simple supervised learning models trained on historical data. However, the use of deep learning, reinforcement learning, or transfer learning [32] could enable more sophisticated and generalizable adaptation strategies that can handle novel attack patterns and rapidly evolving IoT ecosystems.

Another promising direction is integrating our framework with other security mechanisms, such as intrusion detection systems, firewalls, and threat intelligence platforms. By correlating honeypot data with signals from these additional sources, we can achieve a more holistic view of the IoT threat landscape and enable proactive defence measures. This requires the development of standardized data exchange formats and APIs to facilitate interoperability and real-time sharing of threat indicators.

Finally, our framework's evaluation could be further strengthened by conducting more extensive and diverse real-world deployments. While our current evaluation metrics provide a solid foundation, more fine-grained benchmarks that capture the nuances of different IoT application domains and attack scenarios are needed. Collaborating with industry partners and research institutions to establish shared testbeds and datasets would significantly accelerate the validation and refinement of adaptive IoT honeypot solutions.

5. Conclusion

In this paper, we presented "The sweet taste of IoT deception", an integrated framework for the design, implementation, and evaluation of adaptive honeypots in IoT environments. Our framework leverages machine learning techniques to create dynamic, customized deception

environments that can engage attackers and elicit novel attack behaviours. We also proposed an evaluation framework, including a set of quantitative metrics, to assess the effectiveness of IoT honeypots in realistic deployment scenarios.

The main contributions of our work include:

1. The design and implementation of an adaptive honeypot framework that integrates diverse honeypot types and supports intelligent adaptation based on attacker behaviour.
2. The development of an evaluation framework that captures the ability of honeypots to attract, deceive, and contain IoT attackers.
3. A discussion on the current state and future directions of IoT honeypot research, highlighting key challenges and promising solutions.

We also acknowledge several limitations and areas for future improvement. First, more advanced machine learning techniques are needed to handle novel attack patterns and rapidly evolving IoT ecosystems. Second, integration with other security mechanisms and threat intelligence platforms is necessary to enable holistic and proactive defence. Finally, more extensive real-world deployments and collaborations are required to validate and refine the proposed framework across diverse IoT domains.

Future research directions include developing more sophisticated adaptation strategies using deep learning, reinforcement learning, or transfer learning, integrating our framework with other security mechanisms, and establishing shared testbeds and datasets to accelerate the validation and refinement of adaptive IoT honeypot solutions.

However, further research and development are needed to address the identified limitations and fully realize the potential of this technology. In further research, it would be worthwhile to consider the following aspects:

- While the paper discusses real-world challenges, a more detailed analysis of practical implementation and deployment considerations would be beneficial. This could include investigating the scalability and performance of the proposed framework in large-scale IoT networks, as well as the integration with existing security infrastructures and processes.
- A deeper exploration of the potential security implications of deploying honeypots, especially in critical infrastructure, could be valuable. This may involve analyzing the risks associated with honeypot compromise, such as the potential for attackers to use captured honeypots as stepping stones for further attacks and developing strategies to mitigate these risks.
- The ethical implications of using honeypots, particularly in terms of data privacy and potential legal issues, should be addressed. Future research could examine the compliance of honeypot deployments with relevant regulations, such as GDPR, and propose guidelines for ensuring the responsible and transparent use of deception technologies.
- A more detailed comparison of the proposed framework with existing honeypot solutions would help highlight the unique contributions. This could involve conducting a comprehensive survey of state-of-the-art IoT honeypots, evaluating their capabilities and limitations, and demonstrating how the proposed framework advances beyond these solutions in terms of adaptability, intelligence generation, and evaluation metrics.

Acknowledgments

We want to express our sincere gratitude to the reviewers for their insightful comments and suggestions, which have contributed significantly to improving the quality and clarity of this paper. We also extend our thanks to the editors for their valuable guidance and support throughout the review process. Their constructive feedback and dedication have been instrumental in shaping the final version of this manuscript.

References

[1] Abay, N.C., Akcora, C.G., Zhou, Y., Kantarcioglu, M. and Thuraisingham, B., 2019. Using Deep Learning to Generate Relational HoneyData. In: E. Al-Shaer, J. Wei, K.W. Hamlen and C. Wang, eds. *Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings*. Cham: Springer International Publishing, pp.3–19. Available from: https://doi.org/10.1007/978-3-030-02110-8_1.

[2] Ahmed, Y., Beyioku, K. and Yousefi, M., 2024. Securing smart cities through machine learning: A honeypot-driven approach to attack detection in Internet of Things ecosystems. *IET Smart Cities*. Available from: https://doi.org/10.1049/smc2.12084.

[3] Antonioli, D. and Tippenhauer, N.O., 2015. MiniCPS: A Toolkit for Security Research on CPS Networks. *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*. New York, NY, USA: Association for Computing Machinery, CPS-SPC '15, pp.91–100. Available from: https://doi.org/10.1145/2808705.2808715.

[4] Balas, E.G., 2004. Honeynet Data Analysis – A Technique For Correlating Sebek And Network Data. *DFRWS USA 2004: The fourth annual Digital Forensics Research Workshop*. Available from: https://dfrws.org/presentation/honeynet-data-analysis-a-technique-for-correlating-sebek-and-network-data/.

[5] Bringer, M.L., Chelmecki, C.A. and Fujinoki, H., 2012. A Survey: Recent Advances and Future Trends in Honeypot Research. *International Journal of Computer Network and Information Security*, 4(10), p.63–75. Available from: https://doi.org/10.5815/ijcnis.2012.10.07.

[6] Conpot: ICS/SCADA Honeypot, 2024. Available from: https://github.com/mushorg/conpot.

[7] De, S. and Kar, A.K., 2023. Exploring IoT Applications in Industry 4.0—Insights from Review of Literature. In: P.K. Singh, S.T. Wierzchoń, W. Pawłowski, A.K. Kar and Y. Kumar, eds. *IoT, Big Data and AI for Improving Quality of Everyday Life: Present and Future Challenges: IOT, Data Science and Artificial Intelligence Technologies*. Cham: Springer International Publishing, pp.15–38. Available from: https://doi.org/10.1007/978-3-031-35783-1_2.

[8] dionaea, 2021. Available from: https://github.com/DinoTools/dionaea.

[9] Dowling, S., Schukat, M. and Melvin, H., 2017. A ZigBee honeypot to assess IoT cyberattack behaviour. *2017 28th Irish Signals and Systems Conference, ISSC 2017*. Institute of Electrical and Electronics Engineers Inc. Available from: https://doi.org/10.1109/ISSC.2017.7983603.

[10] Farris, I., Taleb, T., Khettab, Y. and Song, J., 2019. A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems. *IEEE Communications Surveys & Tutorials*, 21(1), pp.812–837. Available from: https://doi.org/10.1109/COMST.2018.2862350.

[11] Fawaz, A., Bohara, A., Cheh, C. and Sanders, W.H., 2016. Lateral Movement Detection Using Distributed Data Fusion. *2016 IEEE 35th Symposium on Reliable Distributed Systems (SRDS)*. pp.21–30. Available from: https://doi.org/10.1109/SRDS.2016.014.

[12] Felix, M., Safitri, C. and Mandala, R., 2022. Framework for Analyzing Intruder Behavior of IoT Cyber Attacks Based on Network Forensics by Deploying Honeypot Technology. *ICOIACT 2022 - 5th International Conference on Information and Communications Technology: A New Way to Make AI Useful for Everyone in the New Normal Era, Proceeding*. Institute of Electrical and Electronics Engineers Inc., pp.423–428. Available from: https://doi.org/10.1109/ICOIACT55506.2022.9971886.

[13] Hakim, M.A., Aksu, H., Uluagac, A.S. and Akkaya, K., 2018. U-PoT: A Honeypot Framework for UPnP-Based IoT Devices. *2018 ieee 37th international performance computing and communications conference, ipccc 2018*. Institute of Electrical and Electronics Engineers Inc. Available from: https://doi.org/10.1109/PCCC.2018.8711321.

[14] Huang, L. and Zhu, Q., 2019. Adaptive Honeypot Engagement Through Reinforcement Learning of Semi-Markov Decision Processes. In: T. Alpcan, Y. Vorobeychik, J.S. Baras and G. Dán, eds. *Decision and Game Theory for Security*. Cham: Springer International Publishing, *Lecture Notes in Computer Science*, vol. 11836, pp.196–216. Available from: https://doi.org/10.1007/978-3-030-32430-8_13.

[15] Jony, A.I. and Arnob, A.K.B., 2024. A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset. *Journal of Edge Computing*, 3(1), p.28–42. Available from: https://doi.org/10.55056/jec.648.

[16] Kala, S. and Nalesh, S., 2022. Security and challenges in IoT-enabled systems. In: P. Johri, A. Anand, J. Vain, J. Singh and M. Quasim, eds. *System Assurances*. Academic Press, Emerging Methodologies and Applications in Modelling, chap. 24, pp.437–445. Available from: https://doi.org/10.1016/B978-0-323-90240-3.00024-2.

[17] Kour, K., Goswami, S., Sharma, M., Sivasankar, P.T., Vekariya, V. and Kumari, A., 2022. Honeynet Implementation in Cyber Security Attack Prevention with Data Monitoring System Using AI Technique and IoT 4G Networks. *International Journal of Communication Networks and Information Security*, 14(3), pp.163–175. Available from: https://doi.org/10.17762/ijcnis.v14i3.5603.

[18] Lantz, B., Heller, B. and McKeown, N., 2010. A network in a laptop: rapid prototyping for software-defined networks. *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*. New York, NY, USA: Association for Computing Machinery, Hotnets-IX. Available from: https://doi.org/10.1145/1868447.1868466.

[19] Luo, T., Xu, Z., Jin, X., Jia, Y. and Ouyang, X., 2017. IoTCandyJar: Towards an Intelligent-Interaction Honeypot for IoT Devices. *BlackHat USA*. Available from: https://www.blackhat.com/docs/us-17/thursday/us-17-Luo-Iotcandyjar-Towards-An-Intelligent-Interaction-Honeypot-For-IoT-Devices.pdf.

[20] Lygerou, I., Srinivasa, S., Vasilomanolakis, E., Stergiopoulos, G. and Gritzalis, D., 2022. A decentralized honeypot for IoT Protocols based on Android devices. *International Journal of Information Security*, 21(6), pp.1211–1222. Available from: https://doi.org/10.1007/s10207-022-00605-7.

[21] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J.,

Shenker, S. and Turner, J., 2008. OpenFlow: enabling innovation in campus networks. *SIGCOMM Comput. Commun. Rev.*, 38(2), p.69–74. Available from: https://doi.org/10.1145/1355734.1355746.

[22] Mokube, I. and Adams, M., 2007. Honeypots: concepts, approaches, and challenges. *Proceedings of the 45th Annual ACM Southeast Conference*. New York, NY, USA: Association for Computing Machinery, ACMSE '07, p.321–326. Available from: https://doi.org/10.1145/1233341.1233399.

[23] Morozov, D.S., Vakaliuk, T.A., Yefimenko, A.A., Nikitchuk, T.M. and Kolomiiets, R.O., 2023. Honeypot and cyber deception as a tool for detecting cyber attacks on critical infrastructure. In: T.A. Vakaliuk and S.O. Semerikov, eds. *Proceedings of the 3rd Edge Computing Workshop, Zhytomyr, Ukraine, April 7, 2023*. CEUR-WS.org, *CEUR Workshop Proceedings*, vol. 3374, pp.81–96. Available from: https://ceur-ws.org/Vol-3374/paper06.pdf.

[24] Nawrocki, M., Wählisch, M., Schmidt, T.C., Keil, C. and Schönfelder, J., 2016. A Survey on Honeypot Software and Data Analysis. 1608.06249, Available from: https://arxiv.org/abs/1608.06249.

[25] Oosterhof, M., 2024. Cowrie SSH/Telnet Honeypot. Available from: https://github.com/cowrie/cowrie.

[26] Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C., 2016. IoTPOT: A novel honeypot for revealing current IoT threats. *Journal of Information Processing*, 24(3), pp.522–533. Available from: https://doi.org/10.2197/ipsjjip.24.522.

[27] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M. and Duchesnay Édouard, 2011. Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*, 12(85), pp.2825–2830. Available from: http://jmlr.org/papers/v12/pedregosa11a.html.

[28] Prathapani, A., Santhanam, L. and Agrawal, D.P., 2009. Intelligent honeypot agent for blackhole attack detection in Wireless Mesh Networks. *2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*. pp.753–758. Available from: https://doi.org/10.1109/MOBHOC.2009.5336925.

[29] Provos, N., 2004. A Virtual Honeypot Framework. *13th USENIX Security Symposium (USENIX Security 04)*. San Diego, CA: USENIX Association. Available from: https://www.usenix.org/conference/13th-usenix-security-symposium/virtual-honeypot-framework.

[30] Redwood, O., Lawrence, J. and Burmester, M., 2015. A Symbolic Honeynet Framework for SCADA System Threat Intelligence. In: M. Rice and S. Shenoi, eds. *Critical Infrastructure Protection IX*. Cham: Springer International Publishing, *IFIP Advances in Information and Communication Technology*, vol. 466, pp.103–118. Available from: https://doi.org/10.1007/978-3-319-26567-4_7.

[31] Sayed, M.A., Anwar, A.H., Kiekintveld, C. and Kamhoua, C., 2023. Honeypot Allocation for Cyber Deception in Dynamic Tactical Networks: A Game Theoretic Approach. Available from: https://doi.org/10.48550/arXiv.2308.11817.

[32] Semerikov, S., Zubov, D., Kupin, A., Kosei, M. and Holiver, V., 2024. Models and Technologies for Autoscaling Based on Machine Learning for Microservices Architecture. In: V. Lytvyn, A. Kowalska-Styczen and V. Vysotska, eds. *Proceedings of the 8th International Conference on Computational Linguistics and Intelligent Systems. Volume I: Machine Learning*

Workshop, Lviv, Ukraine, April 12-13, 2024. CEUR-WS.org, *CEUR Workshop Proceedings*, vol. 3664, pp.316–330. Available from: https://ceur-ws.org/Vol-3664/paper22.pdf.

[33] Sokol, P., Míšek, J. and Husák, M., 2017. Honeypots and honeynets: issues of privacy. *EURASIP Journal on Information Security*, 2017(1), p.4. Available from: https://doi.org/10.1186/s13635-017-0057-4.

[34] Spitzner, L., 2002. *Honeypots: Tracking Hackers*. USA: Addison-Wesley Longman Publishing Co., Inc.

[35] Tabari, A.Z., Liu, G., Ou, X. and Singhal, A., 2023. Revealing Human Attacker Behaviors Using an Adaptive Internet of Things Honeypot Ecosystem. In: G. Peterson and S. Shenoi, eds. *Advances in Digital Forensics XIX: 19th IFIP WG 11.9 International Conference, ICDF 2023, Arlington, Virginia, USA, January 30-31, 2023, Revised Selected Papers*. Cham: Springer Nature Switzerland, pp.73–90. Available from: https://doi.org/10.1007/978-3-031-42991-0_5.

[36] Tuptuk, N. and Hailes, S., 2018. Security of smart manufacturing systems. *Journal of Manufacturing Systems*, 47, pp.93–106. Available from: https://doi.org/10.1016/j.jmsy.2018.04.007.

[37] Vasilomanolakis, E., Srinivasa, S., Cordero, C.G. and Mühlhäuser, M., 2016. Multi-stage attack detection and signature generation with ICS honeypots. *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*. pp.1227–1232. Available from: https://doi.org/10.1109/NOMS.2016.7502992.

[38] Vetterl, A. and Clayton, R., 2019. Honware: A Virtual Honeypot Framework for Capturing CPE and IoT Zero Days. *2019 APWG Symposium on Electronic Crime Research (eCrime)*. pp.1–13. Available from: https://doi.org/10.1109/eCrime47957.2019.9037501.

[39] Vishwakarma, R. and Jain, A.K., 2019. A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks. *Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019*. Institute of Electrical and Electronics Engineers Inc., pp.1019–1024. Available from: https://doi.org/10.1109/ICOEI.2019.8862720.

[40] Wang, M., Santillan, S. and Kuipers, F., 2018. ThingPot: an interactive Internet-of-Things honeypot. Available from: https://doi.org/10.48550/arXiv.1807.04114.