RESEARCH PAPER

Design and Implementation of an IoT Honeypot System for Real-Time Cyber Threat Monitoring and Analysis

Mrs. L. Christophel Selvi[1], Guberan V[2], Kavyasri S[3]

[1] Assistant Professor, Department of Electronics and Communication Engineering (ECE), IFET College of Engineering, Villupuram, Tamil Nadu, India. Email: selvilourdusamy@gmail.com
[2] UG Scholar,), IFET College of Engineering, Villupuram, Tamil Nadu, India. Email: guberangrand@gmail.com
[3] UG Scholar, IFET College of Engineering, Villupuram
Mail-id: kavyasri17.ece@gmail.com
Corresponding Author:
Mrs. L. Christophel Selvi[1] (selvilourdusamy@gmail.com)*

ABSTRACT
The exponential growth of the Internet of Things (IoT) has significantly transformed modern technological ecosys-tems by enabling seamless interconnectivity among billions of devices. These devices are widely deployed across various do-mains such as smart homes, healthcare, industrial automation, agriculture, and transportation systems. While IoT has improved efficiency and convenience, it has also introduced critical security challenges due to the lack of robust protection mechanisms in many devices. Most IoT devices are designed with limited com-putational resources, resulting in weak authentication methods, unencrypted communication channels, and infrequent software updates.
Cybercriminals actively exploit these vulnerabilities To get unauthorized access, launch attacks, and build large-scale bot-nets, hackers target IoT devices. Notable botnet-driven DDoS attacks show how much harm these compromised gadgets can inflict. They don't just disrupt services; they also threaten critical infrastructure and data integrity...
Keywords: IoT, Honeypot, Cyber Security, Machine Learn-ing, Real-Time Monitoring, Threat Analysis
How to cite this article: Selvi LC, Guberan V, Kavyasri S. Design and Implementation of an IoT Honeypot System for Real-Time Cyber Threat Monitoring and Analysis. Int J Drug Deliv Technol. 2026;16(61s):1662-1667. DOI: 10.25258/ijddt.16.61s.189
Source of support: *Nil.*
Conflict of interest: Nil.

INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most transformative technological advancements of the 21st century. It enables communication and data exchange between physical devices through the internet, allowing for automation, remote monitoring, and intelligent decision-making. IoT de-vices are now embedded in everyday environments, including smart homes, wearable devices, healthcare systems, industrial control systems, and smart cities.

Despite its rapid adoption, IoT technology presents signif-icant security challenges. Unlike traditional computing sys-tems, IoT devices often have limited processing power, mem-ory, and energy resources. These constraints make it difficult to implement advanced security mechanisms such as encryption, authentication, and intrusion detection.

As a result, many IoT devices are deployed with weak security configurations, including default credentials, open ports, and outdated firmware.

Cyber attackers exploit these vulnerabilities to compromise devices and gain unauthorized access. When IoT devices get
hacked, bad guys can use them to steal data, spy on people, or launch huge cyberattacks. The Mirai botnet is a big example; it took over tons of devices and hit major online services with giant DDoS attacks. Traditional cybersecurity solutions, such as firewalls and intrusion detection systems, are primarily designed to prevent unauthorized access. However, they often lack the ability to provide detailed insights into attacker behavior. Understanding how attackers operate is essential for developing effective defense mechanisms.

In this paper, we propose a low-interaction IoT honeypot system designed to capture and analyze real-world cyber threats. The system integrates service emulation, data logging, machine learning, and real-time visualization to provide com-prehensive threat intelligence. The goal is not only to detect attacks but also to understand attacker behavior and improve IoT security.

Related Work

Honeypots have been widely used in cybersecurity research as a method for detecting and analyzing malicious activities. Honeypots are usually split into low-interaction and high-interaction types. Low-interaction mimics specific services and is easy to set up and manage. High-interaction offers full system access, letting attackers engage more widely, though it's tougher to handle.

*Author for Correspondence: areebakhanam12@gmail.com

TABLE I:COMPARISON OF EXISTING HONEYPOT SYSTEMS

Tool	Type	Protocols	Limitation
Cowrie	Low-interaction	SSH, Telnet	Not IoT-specific
Dionaea	Malware honeypot	Multiple	Limited analytics
Honeyd	Network simulation	TCP/IP	No real-time dashboard
Proposed System	IoT Honeypot	SSH, Telnet, HTTP, MQTT	Improved monitoring

Several tools have been developed for honeypot deployment. Cowrie is a well-known honeypot that simulates SSH and Tel-net services, capturing login attempts and commands executed by attackers. Dionaea is designed to collect malware samples by emulating vulnerable services, while Honeyd allows the creation of virtual network environments for studying attack behavior.

Although these tools are effective in general network environments, they are not specifically designed for IoT systems. IoT devices use unique communication protocols such as MQTT, CoAP, and Zigbee, which are not fully supported by traditional honeypots. Additionally, many existing systems lack real-time monitoring and advanced analytics capabilities. Recent studies have shown that IoT devices are frequently targeted by automated attacks. Attackers use scanning tools to identify vulnerable devices and attempt to gain access using default credentials. These attacks often involve brute-force login attempts, port scanning, and exploitation of known
vulnerabilities.

The proposed system builds upon existing research by focusing specifically on IoT environments. It integrates multi-ple functionalities, including service emulation, real-time data collection, machine learning-based analysis, and visualization. This comprehensive approach enables more effective detection and understanding of IoT-specific threats.

METHODOLOGY

The methodology of the proposed system involves multiple stages, including deployment, data collection, preprocessing, feature extraction, analysis, and visualization. The system is deployed in a virtual environment to ensure isolation and security. Selected ports are exposed to simulate vulnerable IoT devices. Attackers interacting with these ports are redirected to the emulated services. Data collection is performed contin-uously, capturing all relevant information from attacker interactions. This includes IP addresses, login attempts, commands executed, and timestamps.

The collected data is preprocessed to remove duplicates and inconsistencies. Feature extraction is then performed to identify patterns such as login frequency, and port access behavior. A risk scoring mechanism is applied to evaluate the severity of each attack. Machine learning models are trained using the processed data to classify attacks into categories such as brute-force attacks, scanning, and suspicious behavior. The final stage involves visualizing the results through a dashboard and generating alerts for high-risk activities.

A. System Architecture Overview

The proposed IoT honeypot system is designed using a layered architecture that ensures modularity, scalability, and flexibility. Each layer performs a specific function in capturing and analyzing attack data.

The first layer is the network exposure layer, which opens selected ports such as SSH (22), Telnet (23), HTTP (80), and MQTT (1883). These ports are commonly targeted by attackers searching for vulnerable IoT devices.

Fig. 1. Methodology Flow of the Proposed System

The second layer is the service emulation layer, which simulates the behavior of IoT devices. Instead of running actual services, this layer generates fake responses such as login prompts and command-line interfaces. This ensures that attackers remain engaged while preventing any real damage to the system.

The logging layer captures all interactions between attackers and the honeypot. This includes IP addresses, login attempts, commands executed, session duration, and timestamps.

The analysis layer processes the collected data using machine learning algorithms. It classifies attacks into different categories and calculates risk levels based on predefined criteria.

The final layer is the visualization layer, which provides a user-friendly dashboard that displays real-time attack statistics. This enables users to monitor ongoing threats and identify patterns.

The layered design of the proposed system improves maintainability and simplifies future enhancements. Since each layer operates independently, modifications or upgrades can be implemented without affecting the entire system. For example, new communication protocols or attack detection mechanisms can be added to the service emulation or analysis layers with minimal changes to other components. This modular approach increases the adaptability of the system in rapidly evolving IoT environments.

In addition, the architecture supports efficient data flow between layers, ensuring smooth monitoring and analysis of malicious activities. The logging and analysis layers work together to transform raw attack data into meaningful security insights. These insights are then presented through the visu-alization dashboard in an organized manner, helping admin-istrators quickly understand attack trends, identify vulnerable services, and take preventive actions to strengthen IoT network security.

IMPLEMENTATION

The system is implemented using Python due to its flexibility and extensive library support. Flask is used for developing the web-based dashboard, while socket programming is used for service emulation

SSH and Telnet services display fake login prompts, while HTTP simulates a web interface. MQTT connections are monitored to capture IoT-specific interactions.

All captured data is stored in a structured database. Machine learning models such as Random Forest, Decision Tree, and Naive Bayes are used for classification.

The system also includes an alert mechanism that notifies users when high-risk activities are detected.

Fig. 2. Honeypot Dashboard Interface

MATHEMATICAL MODELING

The system uses mathematical models to quantify attacker behavior and assess risk levels.

Let the set of attacks be represented as:

$A = \{a1, a2, a3, \ldots, an\}$ (1)

Attack frequency is the count of attempts from a certain IP address: F (IP).

Port scanning behavior is found by tallying the unique ports accessed: S(IP).

Command severity is calculated based on predefined weights assigned to different commands:

$$CS = \sum \text{severity weights} \quad (2)$$

The overall risk score is given by:

$$R = (\alpha \times F) + (\beta \times S) + (\gamma \times CS) \quad (3)$$

where α, β, and γ are weighting factors.

This model enables the classification of attacks based on their severity levels.

ADVANTAGES OF THE PROPOSED SYSTEM

The proposed IoT honeypot system offers several advantages that make it suitable for real-world deployment. One of the primary benefits is its lightweight design, which allows it to run efficiently even on systems with limited computational resources. This makes it ideal for IoT environments where hardware capabilities are often constrained.

Another important advantage is its ability to perform real-time monitoring. The system continuously captures attacker interactions and displays them through a dashboard, enabling

immediate awareness of potential threats. This helps in proac-tive decision-making and faster response to suspicious activi-ties.

The integration of machine learning enhances the system's ability to classify attacks accurately. By analyzing patterns in attacker behavior, the system can distinguish between different types of threats and assign appropriate risk levels.

Another significant advantage of the proposed system is its capability to collect and store detailed attack data for future analysis. The captured logs, attacker commands, IP addresses, and payload information can be used by researchers and security administrators to study emerging cyber threats and improve defense mechanisms. This not only helps in under-standing attacker behavior but also supports the development of stronger security policies and intrusion detection techniques for IoT networks.

The modular architecture of the system also improves scalability. Additional services and protocols can be easily integrated without affecting the overall functionality. This flexibility allows the system to adapt to evolving IoT environments.

LIMITATIONS OF THE PROPOSED SYSTEM

Despite its effectiveness, the proposed system has certain limitations that must be considered. Since it is a low-interaction honeypot, it only simulates services rather than providing a full operating environment. As a result, it may not capture highly sophisticated or multi-stage attacks.

APPLICATIONS OF IOT HONEYPOT SYSTEM

The proposed IoT honeypot system has several practical applications in cybersecurity and network monitoring. It can be used in research environments to study attacker behavior and understand emerging threat patterns in IoT networks.

In enterprise environments, the system can be deployed as an early warning mechanism to detect unauthorized access attempts. By identifying suspicious activities, organizations can strengthen their security measures.

The system can also be used for educational purposes, helping students and researchers learn about cybersecurity concepts and real-world attack techniques.

Furthermore, government agencies and security organizations can use such systems to collect threat intelligence and monitor large-scale cyber activities targeting critical infrastruc-ture.

PERFORMANCE ANALYSIS

To see how well the system worked, they looked at accuracy, response time, and resource use. They tested the machine learning models with real attack data and then compared how each performed.

Random Forest achieved the highest accuracy of 94.8%, followed by Decision Tree and Naive Bayes. The higher per-formance of Random Forest can be attributed to its ensemble learning approach, which combines multiple decision trees to improve prediction accuracy

The system demonstrated low response time in capturing and logging attacker interactions. Real-time updates in the dashboard ensured that users could monitor threats without delay.

In terms of resource usage, the system maintained low CPU and memory consumption, making it suitable for deployment in resource-constrained environments.

SECURITY RECOMMENDATIONS

Based on the analysis of captured attack data, several security recommendations can be proposed for improving IoT device security.

First, default credentials should be replaced with strong and unique passwords to prevent brute-force attacks. Multi-factor authentication can further enhance security.

Second, unnecessary ports should be closed, and only essential services should be exposed to the network. This reduces the attack surface.

Third, regular firmware updates should be applied to fix known vulnerabilities and improve system security.

Encryption protocols should be used to secure communication between devices and prevent data interception.

Finally, continuous monitoring and deployment of honeypot systems can help in identifying new threats and improving defense mechanisms.

EXPERIMENTAL RESULTS

The system was deployed for a period of 7 to 14 days and recorded approximately 2450 attack attempts.

Analysis of the data revealed that SSH and Telnet were the most frequently targeted services. Most attacks involved brute-force login attempts using commonly used usernames and passwords.

Machine learning models were evaluated based on their classification accuracy. Random Forest achieved the highest accuracy of 94.8%, followed by Decision Tree and Naive Bayes.

The system demonstrated effective real-time monitoring and classification with minimal resource usage.

The experimental results also showed that the proposed hon-eypot system was capable of identifying different categories of malicious activities, including unauthorized login attempts, command injection attacks, and automated bot scanning. The real-time dashboard successfully visualized attack frequency, source IP activity, and protocol-specific threats, allowing con-tinuous monitoring of attacker behavior. These results confirm that the system can effectively operate as a lightweight and efficient security solution for detecting and analyzing cyber threats in IoT environments.

TABLE II:MACHINE LEARNING MODEL PERFORMANCE

Model	Accuracy	Precision	Recall
Random Forest	94.8%	93.5%	92.6%
Decision Tree	91.4%	90.2%	89.8%
Naive Bayes	87.3%	85.9%	84.7%

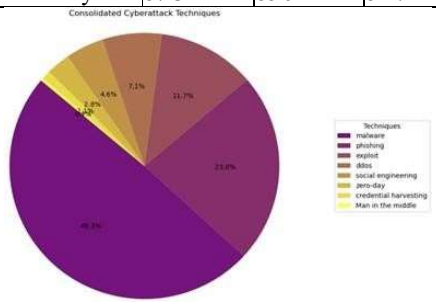

Fig. 3. Attack Distribution by Protocol

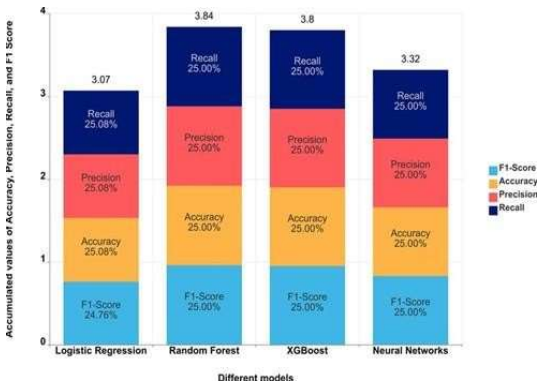

Fig. 4. Comparison of Model Accuracy

DISCUSSION

The experimental results clearly indicate that IoT devices are continuously exposed to automated cyber threats. The high frequency of brute-force login attempts suggests that attackers rely heavily on default credentials and weak authentication mechanisms to gain access. This observation highlights a major security weakness in many real-world IoT deployments. Another important observation from the collected data is the repetitive nature of attack patterns. Many attackers use automated scripts or bots that repeatedly attempt login combi-nations across multiple ports. This confirms that a significant portion of IoT attacks are not manual but automated and

scalable in nature.

The system also revealed that certain ports, particularly SSH and Telnet, are more frequently targeted than others. This is

because these services are commonly exposed in IoT devices and are often misconfigured.

The integration of machine learning plays a crucial role in improving the effectiveness of the system. By analyzing patterns in login attempts, command execution, and access frequency, the system is able to classify attacks with high accu-racy. Among the evaluated models, Random Forest performed the best due to its ability to handle complex and non-linear data patterns.

Another key advantage of the proposed system is its ability to provide real-time monitoring. The dashboard allows users to

observe ongoing attacks, identify suspicious IP addresses, and understand attack trends. This real-time visibility is essential for proactive cybersecurity management.

However, the system also has certain limitations. Since it is a low-interaction honeypot, it only simulates services and does not allow deep interaction with attackers. As a result, it may not capture advanced attack techniques or zero-day exploits. Additionally, the system relies on predefined rules and training data, which may limit its ability to detect completely new attack patterns.

Despite these limitations, the system provides valuable insights into attacker behavior and serves as an effective tool for IoT threat monitoring. It can be further enhanced by integrating more advanced analytics and expanding protocol support.

CONCLUSION

This paper presented the design and implementation of a low-interaction IoT honeypot system for real-time cyber threat monitoring and analysis. The proposed system successfully simulates commonly targeted IoT services such as SSH, Tel-net, HTTP, and MQTT, enabling it to attract attackers and capture valuable interaction data.

The system demonstrated its effectiveness in collecting real-world attack data, including login attempts, command execution patterns, and access frequency. The analysis of this data revealed that IoT devices are continuously targeted by automated attacks, particularly brute-force login attempts and port scanning activities.

The integration of machine learning techniques significantly enhances the system's ability to classify attacks and assess risk levels. Among the models evaluated, Random Forest achieved the highest accuracy, demonstrating its suitability for cybersecurity applications involving complex data patterns.

One of the key strengths of the proposed system is its lightweight and scalable design. It can be easily deployed in various environments without requiring significant computa-tional resources. The real-time dashboard and alert mechanism further improve usability by providing immediate insights into ongoing threats.

In addition to its practical applications, the system con-tributes to cybersecurity research by providing a framework for studying attacker behavior in IoT environments. The insights gained from this system can help in developing more effective defense mechanisms and improving the overall security of IoT networks.

Overall, the proposed IoT honeypot system serves as a valuable tool for threat monitoring, analysis, and awareness. It highlights the importance of proactive security measures in addressing the growing challenges of IoT cybersecurity

.

REFERENCE

1. N. Provos and T. Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison-Wesley, 2007.
2. L. Spitzner, Honeypots: Tracking Hackers, Addison-Wesley, 2002.
3. M. Antonakakis et al., "Understanding the Mirai Botnet," in Proc. USENIX Security Symposium, 2017, pp. 1093–1110
4. S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
5. A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," IEEE Transactions on Emerging Topics in Comput-ing, vol. 5, no. 4, pp. 586–602, 2017.
6. 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.
7. F. M. A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.
8. J. Granjal, E. Monteiro, and J. Sa´ Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.
9. K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in Proc. International Conference on Computational Intelligence and Security, 2013, pp. 663–667.
10. D. B. Rawat and C. Bajracharya, "Cyber Security for Smart Grid Systems: Status, Challenges and Perspectives," in Smart Grid Security, Springer, 2015, pp. 3–19.
11. Y. Meidan et al., "Detection of Unauthorized IoT Devices Using Machine Learning Techniques," IEEE Transactions on Industrial Infor-matics, vol. 14, no. 6, pp. 2736–2746, 2018.
12. S. Marchal, J. Francois, R. State, and T. Engel, "Proactive Discovery of Botnets Using Honeypots," in Proc. IFIP/IEEE International Symposium on Integrated Network Management, 2015, pp. 1–9.
13. K. L. Lueth, "State of the IoT 2020: 12 Billion IoT Connections," IoT Analytics, 2020.

14. A. V. Dastjerdi and R. Buyya, "Fog Computing: Helping the Internet of Things Realize Its Potential," Computer, vol. 49, no. 8, pp. 112–116, 2016.
15. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities," Future Generation Computer Systems, vol. 78, pp. 544–546, 2018..
.