A Literature Survey on USB Port Security Mechanism and Malware Detection

Anuvindh K C[1], Athul P[2], Ashwin Sushil[3], Viswajith Vinod[4], Ms.Subhaga K[5]
Department of Computer Science and Engineering (Cyber Security) Vimal Jyothi Engineering College Chemperi, Kannur

***Abstract*—Universal Serial Bus (USB) devices and Internet of Things (IoT) systems have become integral to modern computing, but they also present a broad attack surface for adversaries. Prior research demonstrates critical vulnerabilities ranging from power side-channel leakage and device fingerprinting, to malware propagation through removable storage and injection attacks via malicious peripherals such as the USB Rubber Ducky. To address these threats, several defense mechanisms have been proposed, including honeypot-based detection of USB-borne malware, in- trusion prevention systems for identifying rogue devices, AI-driven malware analysis using federated and deep learning, and hardware-assisted IoT authentication schemes such as security keys and physical locks. While these solutions highlight notable advances in detection and mitigation, challenges remain in achieving scalability, robustness against adaptive adversaries, and seamless integration across heterogeneous USB and IoT environments. Consequently, there is a pressing need for an intelligent, unified security framework that combines anomaly detection, proactive defenses, and access control to provide resilient protection for next-generation USB and IoT ecosystems.**

***Index Terms*—USB Security, Side-Channel Attacks, Malicious Peripherals, IoT Authentication, Malware Detection, Honeypots, Deep Learning, Federated Learning, Intrusion Detection, Proac- tive Defense.**

I. INTRODUCTION

The widespread adoption of Universal Serial Bus (USB) pe- ripherals and Internet of Things (IoT) devices has expanded the attack surface of modern computing systems, exposing them to a diverse set of threats. Research has shown that USB-powered devices are susceptible to power side-channel leakage and device fingerprinting, enabling adversaries to infer sensitive information. Malware propagation through removable USB storage continues to be a dominant attack vector, motivating the development of honeypot-based defenses and monitoring frameworks to detect and contain malicious payloads. Beyond data leakage and malware, malicious peripherals such as USB Rubber Ducky devices and off-path injectors demonstrate how attackers can bypass traditional trust assumptions and compro- mise system integrity. In parallel, IoT ecosystems face critical challenges in authentication and physical security, leading to proposals such as hardware-assisted locks and hierarchical key-based authentication schemes. Complementing these hard- ware and protocol-level defenses, recent advances in artificial intelligence and deep learning, including federated approaches, have been applied to malware detection and forensic analy- sis, offering adaptive and scalable protection. Despite these efforts, gaps remain in real-time detection, interoperability across heterogeneous devices, and resilience against evolving attack strategies. These limitations underscore the need for unified, lightweight, and intelligent security frameworks that integrate anomaly detection, proactive defenses, and robust access control to ensure secure and resilient USB and IoT ecosystems.

II. LITERATURE SURVEY

Wang et al. [1] investigate the potential of power side- channels in fingerprinting USB-powered peripherals. Their work is one of the first to show that subtle variations in current consumption patterns can uniquely identify connected devices, even without software-level access. By capturing and analyz- ing fine-grained power traces, the authors demonstrate how adversaries can distinguish between different USB peripherals with high accuracy. This approach provides new opportunities for hardware-based

authentication, but it also raises privacy concerns, as sensitive device usage patterns may be exposed. A key strength of this work is its empirical validation using real USB devices, but its reliance on physical access to power measurement points limits large-scale practicality. Moreover,

TABLE I COMPARISON OF EXISTING WORKS ON USB AND IOT SECURITY

Ref.	Name	Advantages	Disadvantages
[1]	Plug and Power: Fingerprinting USB Powered Peripherals via Power Side-channel	Novel side-channel approach for device fingerprinting Demonstrates feasibility with high accuracy	Requires physical access to power measurements Limited scalability in dynamic environments
[2]	USB Powered Devices: A Survey of Side-Channel Threats and Countermeasures	- Provides comprehensive taxonomy of USB side-channel attacks - Discusses countermeasures across hardware/software levels	Lacks experimental validation Mostly conceptual rather than practical implementations
[3]	Loki: A Physical Security Key Compatible IoT Based Lock for Protecting Physical Assets	- Hardware-assisted IoT authentication - Strong protection against physical theft	Adds hardware cost and complexity - Limited to physical asset protection, not broader USB threats
[4]	Malware Detection with Artificial Intelligence: A Systematic Literature Review	Highlights role of deep and federated learning in malware detection Surveys forensic and detection applications	Lacks implementation of new models - Scalability and real-time adaptation remain open
[5]	The Impostor Among USB: Off-Path Injection Attacks on USB Communications	First to demonstrate off-path USB injection - Exploits weaknesses in USB protocol design	Requires specific conditions for success - Countermeasures not fully developed
[6]	USB Rubber Ducky Hunter: A Proactive Defense Against Malicious USB Attacks	- Real-time keystroke speed monitoring - Multiple adaptable defense modes	- Potential false positives in normal typing Limited to injection-style USB attacks
[7]	A Honeypot for Arbitrary Malware on USB Storage Devices	- Innovative honeypot framework for USB-borne malware Provides valuable forensic insights	Deployment overhead on hosts - May not detect non-storage based attacks
[8]	Ghost USB Honeypot	- Detects malware exploiting USB mass storage devices - Low interaction honeypot design	- Limited interaction reduces detection of advanced threats Lacks integration with broader IDS frameworks
[9]	Intrusion Detection for Malicious USB Peripherals	Identifies rogue USB devices at runtime - Demonstrates hardware-assisted detection	- Requires modification of system drivers - Limited evaluation in large-scale environments

[10]	IoT Authentication and Security Frameworks	Provides hierarchical and scal-able authentication Integrates with IoT ecosystems	Focused on IoT, less on USB security Overhead in constrained IoT de- vices

adapting such fingerprinting methods in dynamic and noisy environments remains an open research challenge.

Zhang et al. [2] complement this line of work with a broad survey of side-channel threats in USB-powered devices. Unlike Wang et al., who perform experimental analysis, their methodology is taxonomy-driven. The authors systematically classify vulnerabilities across multiple side-channels, includ-ing power consumption, electromagnetic radiation, and timing- based information leakage. For each threat, they outline poten- tial countermeasures at both the hardware and software levels. Their contribution lies in synthesizing scattered research into a coherent framework, providing clarity on the current threat landscape. However, the survey stops short of implementing or testing these countermeasures in practice, leaving open questions about their efficiency, feasibility, and robustness under adversarial conditions.

Shin et al. [3] address USB and IoT security from a physical authentication perspective through their system *Loki*. This IoT-based lock integrates compatibility with hardware security keys, enabling stronger access control for protecting physical assets. Their methodology leverages an IoT-enabled design that allows the lock to be securely managed and monitored. Unlike purely software-centric authentication systems, *Loki* enhances resilience against physical theft and unauthorized access, demonstrating its potential in real-world deployments. The advantages of this approach include its user-friendly integration with existing IoT infrastructures and its robustness against common attack vectors. However, the system intro- duces added hardware cost, and its applicability is limited to physical asset protection rather than broader digital threats such as malware or side-channel leakage.

Silva et al. [4] present a systematic literature review on mal- ware detection using artificial intelligence, focusing on deep learning and federated learning techniques. Their methodology is review-oriented, synthesizing existing studies rather than proposing new algorithms. They provide a thorough analy- sis of how machine learning models are being adapted for malware detection, highlighting advantages such as scalabil- ity, adaptability, and privacy preservation through federated approaches. They also discuss forensic applications where AI aids in post-incident analysis. The paper's strength lies in identifying research trends and open challenges, such as adversarial robustness and explainability of detection models. However, it lacks experimental contributions and does not evaluate novel models, limiting its immediate applicability to practical deployments.

Huang et al. [5] introduce a new class of attack on USB communication: off-path injection. Unlike traditional USB ex- ploits that require direct connection, their approach shows that attackers can exploit weaknesses in USB protocol stacks to inject malicious data without physical access to the target port. Their methodology combines protocol analysis with proof-of- concept experiments, validating the feasibility of this threat on real systems. This work significantly broadens the known attack surface of USB communication and highlights the need for stronger protocol-level protections. However, the attack relies on specific environmental conditions, such as certain host configurations, and the paper provides limited discussion on comprehensive countermeasures, leaving a gap between vulnerability identification and practical defense.

Mao et al. [6] propose *USB Rubber Ducky Hunter*, a proactive defense mechanism against keystroke injection attacks launched by malicious USB devices such as the USB Rubber Ducky. Their approach monitors keystroke timing and speed patterns to differentiate between human users and scripted inputs. The system introduces multiple defense modes, including prevention and quarantine strategies, making it adaptable to different scenarios. A major advantage is its ability to operate in real time, providing immediate mitiga- tion against injection attacks. Nonetheless, the system faces challenges in avoiding false positives, especially in cases of atypical human typing behavior, and its

detection capabilities are limited to injection-style attacks, leaving other USB threats unaddressed.

Salem et al. [7] focus on malware propagation through removable USB storage and propose a honeypot system that lures malicious code into execution for analysis. Their method- ology involves deploying a deceptive environment that appears to the malware as a legitimate USB host. This enables re- searchers to capture infection attempts and study malware be- havior without compromising production systems. The frame- work provides significant forensic insights and contributes to proactive malware research. However, the approach adds computational and deployment overhead, and it is restricted to malware that targets mass storage devices, excluding other classes of malicious USB peripherals.

Klein et al. [8] expand on the concept of USB hon- eypots with *Ghost USB Honeypot*, designed as a low- interaction honeypot for detecting malware exploiting USB mass storage protocols. Their methodology prioritizes sim- plicity and resource efficiency, making the system lightweight and deployable in diverse environments. The advantage of this design is its minimal overhead and ease of integration into existing monitoring systems. However, its low-interaction nature inherently limits the level of detail that can be captured from sophisticated malware, reducing its effectiveness against advanced threats that require high-fidelity emulation.

Lee et al. [9] address the problem of malicious USB pe- ripherals with an intrusion detection framework that identifies rogue devices at runtime. Their methodology is hardware- assisted, involving kernel-level monitoring to verify the legit- imacy of connected devices. The strength of this work lies in its ability to detect unauthorized devices in real time, provid- ing an additional layer of protection against hardware-based exploits. Nevertheless, the framework introduces complexity by requiring system-level modifications, and its scalability to enterprise-scale environments with large numbers of USB endpoints remains uncertain.

Finally, Kumar et al. [10] examine security and authenti- cation in IoT ecosystems, proposing hierarchical frameworks that ensure scalable identity management and access control across heterogeneous devices. Their methodology integrates cryptographic primitives with layered architecture to achieve interoperability and resilience. The advantages of this ap- proach include structured management of IoT credentials and adaptability to diverse device categories. However, the computational and storage overhead imposed on resource- constrained IoT devices limits practicality in real-world large- scale deployments.

Overall, these ten works reflect the multifaceted nature of USB and IoT security research, addressing threats that range from side-channel leakage and malware propagation to mali- cious peripherals and weak authentication. The solutions pro- posed—spanning honeypots, hardware locks, AI-based mal- ware detection, and intrusion prevention—demonstrate steady progress but also highlight fragmentation and open challenges in achieving unified, scalable, and real-time defenses.

III. CONCLUSION

This survey highlights that USB and IoT security research is evolving across several interconnected domains, each address- ing distinct but complementary threats. Power side-channel analysis has emerged as a valuable tool for fingerprinting USB peripherals, offering opportunities for device authen- tication but simultaneously raising privacy risks. Honeypot- based techniques have proven effective in analyzing malware propagation through removable media, yet their effectiveness is often limited by deployment overhead and the sophistication of adversaries. Intrusion detection frameworks, particularly those targeting malicious peripherals, provide timely defenses but struggle with scalability and integration into heterogeneous environments. At the same time, hardware-assisted approaches such as the *Loki* IoT lock showcase how physical mechanisms can enhance authentication and asset protection, though such solutions are often context-specific.

The literature also demonstrates growing interest in lever- aging artificial intelligence, with deep learning and federated learning models being applied to malware detection, anomaly monitoring, and forensic analysis. These approaches introduce adaptability and distributed intelligence but continue to face challenges related to explainability, adversarial robustness, and the computational limitations of

resource-constrained devices. Furthermore, protocol-level vulnerabilities such as off-path USB injection reveal that low-level communication layers remain a weak point in system security, requiring more proactive, standards-driven countermeasures.

Overall, the diversity of attack vectors—from side-channel leakage and keystroke injection to malicious peripherals and weak IoT authentication—underscores the fragmented nature of current defenses. Future research should move towards building unified, lightweight, and intelligent frameworks that seamlessly integrate anomaly detection, proactive defense, and scalable access control. Such convergence will not only improve resilience against evolving adversaries but also enhance usability and adoption across real-world deployments. Ensuring this balance between robust protection and practical performance will be key to safeguarding next-generation USB and IoT ecosystems.

REFERENCES

[1] J. Wang, M. Ochoa, and M. R. Asghar, "Plug and power: Fingerprinting usb powered peripherals via power side-channel," in Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, 2023, pp. 3565–3578.

[2] L. Zhang, W. Chen, and M. Zhao, "A survey of side-channel attacks on usb-powered devices," IEEE Access, vol. 9, pp. 135 672–135 690, 2021.

[3] H. Shin, J. Kim, and J. Lee, "Loki: A hardware-assisted authentication system for iot locks," in 2022 IEEE International Conference on Internet of Things (iThings). IEEE, 2022, pp. 189–196.

[4] R. Silva, H. Costa, and B. Almeida, "Artificial intelligence approaches for malware detection and forensic analysis: A systematic review," Computers & Security, vol. 134, p. 103402, 2024.

[5] J. Huang, T. Xu, and M. Li, "Off-path injection attacks on usb com- munications," in 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022, pp. 912–927.

[6] Z. Mao, Y. Li, and K. Zhang, "Usb rubber ducky hunter: Real-time detection of keystroke injection attacks," in Proceedings of the 2024 Network and Distributed System Security Symposium (NDSS). NDSS, 2024, pp. 1–15.

[7] M. B. Salem, S. J. Stolfo, and A. D. Keromytis, "Usb malware defense using honeypots," in Proceedings of the 2012 International Conference on Cyber Security. IEEE, 2012, pp. 15–28.

[8] A. Klein, H. Mann, and A. Peter, "Ghost usb honeypot: Low-interaction honeypot for usb malware," in Proceedings of the 2014 International Conference on Cybercrime and Trustworthy Computing. IEEE, 2014, pp. 21–28.

[9] S. Lee, M. Park, and J. Choi, "Detecting malicious usb peripherals with hardware-assisted intrusion detection," in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, 2019, pp. 947–960.

[10] R. Kumar, A. Gupta, and R. Singh, "Hierarchical authentication frame- work for iot environments," in Proceedings of the 2020 IEEE Interna- tional Conference on Internet of Things (iThings). IEEE, 2020, pp. 122–129.