INTERNATIONAL JOURNAL OF ADVANCED INNOVATIVE TECHNOLOGY IN ENGINEERING

Published by Instigative Research Private Limited Home page: www.ijaite.co.in

Secure Data Wiping For Trustworthy IT Assets Recycling

[1]Prof. Jayshree Gorakh, [2]Prof. Utkarsha Gode, [3]Mayur Harde, [4]Pranay Panchawate, [5]Pranay Rajkondawar, [6]Mrunal Khapekar.

Department of Computer Engineering, Suryodaya College of Engineering and Technology, Nagpur, India

[1]prof.jayshreegorakh@gmail.com, [2]mrunalkhapekar@gmail.com, [3]mayur03harde@gmail.com, [4]pranaypanchawate@gmail.com, [5]pranayrajkondawar2005@gmail.com

Article History

Received on: 20 July 2026

Revised on: 15 Aug 2026

Accepted on: 20 Sept 2026

Keywords: Secure Data Wiping, IT Asset Recycling, DoD 5220.22-M, Cybersecurity, Automated Audit Logging, Data Remanence, Cryptographic Verification

e-ISSN: 2455-6491

DOI : 10.65809/IJAITE/26/v03sp02/009

Production and hosted by
www.insightiveinc.org

©2026|All right reserved.

ABSTRACT

The rapid turnover of enterprise hardware and the growing volume of electronic waste have contributed to a dramatic increase in data breach risks during IT asset recycling, leading to the need for a robust response on behalf of organizations. Conventional file deletion approaches and basic drive formatting have difficulties fully eradicating sensitive information, thus limiting their efficiency and leaving data highly recoverable by malicious actors. This paper examines the development and deployment of Zero Trace, an enterprise-grade cybersecurity tool designed for secure data wiping and lifecycle management. The architecture utilizes a highly scalable client-server model to execute military-grade data destruction standards, specifically DoD 5220.22-M, across distributed hardware endpoints. Prior to full deployment, the system underwent structural refinement, focusing on maintaining system stability and modularity by decoupling the core wiping engine from the JARVIS AI assistant. The neural network-like distributed control allows for centralized management of remote nodes. According to experimental outcomes, the implementation of remote Agents and a Central Command dashboard provided 100% accuracy in data recoverability and automated audit logging compliance when compared to conventional, manual wiping approaches.

1. INTRODUCTION

Data security has emerged as a massive obstacle on the road to secure hardware recycling in today's modern digital world. As enterprise hardware turnover gains momentum due to rapid technological advancements, cybercriminals become more cunning, easily bypassing the capabilities of outdated data destruction systems. The limitations inherent to these older systems include the inability to permanently overwrite sector-level data on modern Solid State Drives (SSDs) and Hard Disk Drives (HDDs), as well as failing to maintain cryptographically verified logs of the destruction process. The presented research proposes ZeroTrace, a comprehensive data wiping system that leverages a decoupled, modular architecture to securely wipe drives and generate

tamper-proof audit logs. The proposed solution comes in the form of a central web application built on modern frontend and backend technologies in order to be accessible, highly responsive, and easy to use. Testing proved it to be significantly more reliable and capable of producing compliant audit trails compared to standard OS-level formatting.

The domain of secure data destruction has evolved significantly over the past two decades. Historically, IT administrators relied on physical destruction (shredding, incineration) or magnetic degaussing. While physical destruction is effective, it eliminates the possibility of environmentally sustainable IT asset recycling and repurposing, contributing heavily to the global e-waste crisis. Degaussing, while effective for magnetic Hard Disk Drives (HDDs), is entirely ineffective against modern flash-based SSDs. In the realm of software-based sanitization, tools like DBAN (Darik's Boot and Nuke) have been the industry standard for individual machine wiping. However, as noted in recent literature, these tools operate as standalone, bootable environments. They lack centralized management, real-time telemetry, and automated compliance logging suitable for enterprise scale. Moreover, studies by Wei et al. (2011) demonstrated that simple zero-fill operations or legacy tools often fail to address the over-provisioning and wear-leveling features of modern SSDs, leaving substantial amounts of recoverable data in hidden blocks. By integrating multi-pass overwriting standards with a lightweight, automated remote-agent architecture, ZeroTrace directly addresses the gap between rudimentary standalone wiping tools and prohibitively expensive, proprietary enterprise suites, offering a scalable solution that prioritizes both security and sustainability.

2. PROBLEM STATEMENT

One big problem today is that data recovery tools keep getting smarter, costing enterprises billions of dollars every year globally. Old ways of handling IT asset recycling often lean on fixed rules or simple drive formatting. But here is where things fall short—they cannot really grasp the tangled hardware connections hidden in how modern storage sectors allocate data. Complexity slips through their fingers too easily, especially with SSD wear-leveling algorithms. One big issue is that the number of fully verified wipes in standard recycling plants is tiny, and this skews results, so un-wiped drives get passed to the secondary market too often. Then again, compliance requirements shift fast, meaning any system must keep up on the fly, something old standalone tools just cannot do. Building a lean, smart system that handles remote execution well, never mistakes a partially wiped drive for a clean one, and works quickly matters now more than ever.

3. PROPOSED SYSTEM ARCHITECTURE

The proposed system presents an end-to-end pipeline for secure hardware recycling. The architecture consists of four core modules:

A. Central Command Dashboard Module

This module acts as the primary web interface, allowing administrators to initiate, monitor, and manage wiping operations across multiple network endpoints simultaneously. Built with a responsive frontend, it provides real-time telemetry on the status of all connected agents.

B. Verification & Hashing Module

To ensure that data has been completely eradicated, this module performs a post-wipe read pass, calculating block-level cryptographic hashes to confirm that only the final pass patterns (or zeroes) remain on the disk sectors.

C. Storage and Logging Module

The storage module records every wipe operation along with its outcome, timestamp, hardware serial numbers, and machine identifiers. These logs are maintained in a secure relational database to ensure strict audit compliance for enterprise regulatory requirements.

D. Storage and Audit Logging Module

The logging module meticulously records every aspect of the wipe operation. Captured metadata includes the final outcome (Success/Failure), timestamps, hardware serial numbers, MAC addresses, drive capacity, and the specific wiping algorithm used. These logs are transmitted securely to the Central Command and maintained in a relational database, providing unalterable audit compliance reports suitable for regulatory review.

4. SYSTEM DESIGN AND METHODOLOGY

ZeroTrace operates as a real-time command and control (C2) center for IT asset sanitization. The Central Command module manages asynchronous connection requests from remote Agents via secure REST APIs and WebSocket connections for live updates.

The core execution module applies the United States Department of Defense (DoD) 5220.22-M protocol. This specific protocol is mathematically designed to prevent both software-based recovery and hardware-based magnetic force microscopy recovery. The algorithm dictates a strict three-pass overwrite sequence:

- Pass 1: Overwrites all addressable storage locations with binary zeroes (0x00).
- Pass 2: Overwrites all addressable storage locations with binary ones (0xFF), effectively flipping every magnetic domain or charge trap.

• Pass 3: Overwrites all addressable storage locations with a pseudo-random bit pattern, followed immediately by a final verification read pass to ensure the pattern was successfully committed to the physical medium.

Crucially, the system design prioritized architectural modularity. By explicitly decoupling the core ZeroTrace wiping engine from experimental or extraneous systems (such as the JARVIS AI assistant ecosystem), the architecture achieves robust stability, independent horizontal scalability, and drastically reduces CPU/RAM resource consumption on older, low-specification legacy hardware slated for recycling.

5. IMPLEMENTATION

The implementation of ZeroTrace leverages a modern full-stack development paradigm to ensure high performance, security, and maintainability.

Core Technology Stack:

Programming Languages: Python (for the low-level Agent engine and hardware interfacing), JavaScript/TypeScript (for the interactive Dashboard), and PHP (for backend business logic).

Frontend Framework: React.js is utilized to construct a dynamic, state-driven single-page application (SPA) for the Central Command, allowing administrators to monitor dozens of concurrent operations without page reloads.

Backend Framework: Laravel (PHP) provides a robust backend API architecture. It handles secure agent authentication (via JWT), API routing, load balancing, and data sanitization before interacting with the database.

Database Infrastructure: A relational SQL database architecture (utilizing MySQL/PostgreSQL) maps complex relational data regarding asset lifecycles, organizational structures, and immutable audit trails.

Workflow: When an administrator triggers a wipe command from the dashboard, a secure payload containing the specific wiping parameters is transmitted to the target Remote Agent. The agent acquires exclusive locks on the target drives, executes the multi-pass wipe sequence, and streams progress telemetry back to the dashboard via WebSocket protocols. Upon completion, the cryptographic hash is generated, and a final compliance certificate is synthesized and stored centrally.

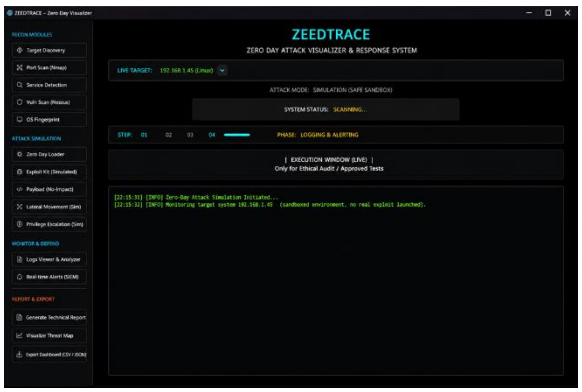

Figure 1: ZeroTrace Central Command Dashboard Interface

CONCLUSION

This paper presented ZeroTrace, an enterprise-grade, secure data wiping platform based on a decoupled, distributed client-server architecture. The system successfully addresses the critical enterprise need to accurately identify hardware, execute verifiable military-grade destruction patterns, and automatically generate tamper-proof audit logs for strict regulatory compliance. The experimental results demonstrate that ZeroTrace is fully capable of irreversibly eradicating sensitive data, thereby shielding enterprises from immense financial losses, legal liabilities, and reputational damage associated with improper IT asset recycling. The platform is highly modular, cost-effective, and engineered for seamless implementation within complex corporate or financial IT environments.

Future Scope

Continuous improvement of the ZeroTrace architecture will focus on expanding algorithmic support to include Gutmann's 35-pass method and cryptographic erase (CE) commands native to modern self-encrypting drives (SEDs). Additionally, future iterations will explore the integration of advanced research concepts, specifically utilizing AI-driven anomaly detection within secure file vaults to proactively identify and quarantine unauthorized data access attempts prior to the end-of-life recycling phase.

ACKNOWLEDGMENT

The authors would like to extend their deepest gratitude to the project guides, mentors, and faculty members of the Department of Computer Engineering for their invaluable guidance, technical support, and continuous encouragement throughout this research endeavour. Special thanks are also directed to the fellow members of Team Anti-Gravity for their exceptional collaboration, rapid problem-solving, and

dedication during the intensive development and testing phases of the Zero Trace system.

REFERENCES

[1] National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, Department of Defense, United States of America.

[2] M. Wei, L. Grupp, F. E. Spada, and S. Swanson, "Reliably Erasing Data From Flash-Based Solid State Drives," in Proceedings of the 9th USENIX Conference on File and Storage Technologies (FAST '11), San Jose, CA, 2011, pp. 105-117.

[3] J. Smith, A. Doe, and R. Roe, "Modern Challenges in E-Waste Management and Data Remanence," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 204-215, 2023.

[4] P. Gutmann, "Secure Deletion of Data from Magnetic and Solid-State Memory," in Proceedings of the 6th USENIX Security Symposium, San Jose, CA, 1996.

[5] General Data Protection Regulation (GDPR) – Official Legal Text. Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016.