International Journal of Web of Multidisciplinary Studies
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
website: https://ijwos.com OPEN ACCESS E-ISSN : 3049-2424
Volume 3 Issue 3 , March 2026
DOI: https://doi.org/10.71366/ijwos03032651788

# SECURE DATA WIPING FOR IT ASSET RECYCLING

P. KRISHNAVENI[1], ARUN KUMAR .A[2], A.BOOPATHY[3], THIRUMALAI RAJ S[4]
[1] *Assistant Professor, Department of Information Technology , M P Nachimuthu M Jaganthan Engineering College*
[2,3,4] *Final Year B.Tech (IT), Department of Information Technology , M P Nachimuthu M Jaganthan Engineering College.*

***Article Info***

***Article History:***

*Published:19 March 2026*

***Publication Issue:***
*Volume 3, Issue 3*
*March-2026*

***Page Number:***
*410-414*

***Corresponding Author:***
*P. KRISHNAVENI*

***Abstract:***

The rapid growth of information technology has increased the number of obsolete IT assets such as laptops, servers, solid-state drives (SSDs), and hard disks. When organizations recycle or dispose of these devices, sensitive data may remain stored in the storage media, leading to potential data breaches and privacy violations. Improper data destruction and the absence of verifiable wiping mechanisms pose serious security risks for enterprises. This research proposes a secure platform named Secure Asset Wiper, which provides reliable data wiping, device tracking, and audit verification for IT asset recycling processes. The proposed system integrates microservices, Next.js, and MySQL database to create a scalable web-based platform. A Java-based Local Agent enables communication between hardware storage devices and the web system, allowing disk scanning and secure wiping operations. The platform supports multiple data wiping standards including NIST 800-88 and DoD 5220.22-M, ensuring compliance with international data destruction guidelines. Real-time monitoring of wipe progress is implemented using WebSocket communication, allowing administrators to track wiping operations instantly. The system also includes multi-tenant architecture, role-based authentication, and audit logging to ensure enterprise-grade security. Experimental evaluation demonstrates that the platform successfully provides reliable data destruction, device monitoring, and verifiable wipe logs, making it suitable for enterprise-scale IT asset recycling management.

***Keywords:*** Data wiping, IT asset recycling, cybersecurity, microservices architecture, secure data destruction, device management

## 1. INTRODUCTION

With the rapid advancement of information technology, organizations frequently upgrade and replace their IT infrastructure, resulting in a large number of obsolete or decommissioned devices. These devices include laptops, servers, hard drives, and solid-state drives that often contain sensitive organizational data. When devices are recycled or sold without proper data destruction procedures, confidential information may be exposed, leading to serious security breaches and compliance violations. Traditional data deletion techniques such as simple file deletion or disk formatting are insufficient to permanently remove stored information.

Advanced data recovery tools can easily retrieve deleted files, posing a major risk to organizations that handle sensitive data such as financial records, personal information, and intellectual property. To address these challenges, secure data wiping methods have been developed to overwrite storage sectors multiple times using

standardized algorithms. However, many organizations still lack centralized systems to manage device tracking, verify wiping operations, and maintain audit logs for compliance verification.

This research proposes a Secure Data Wiping Platform for IT Asset Recycling that integrates device scanning, secure data destruction, real-time monitoring, and enterprise-level management features into a unified system. The proposed architecture combines web technologies and hardware-level device access through a local agent, enabling organizations to securely erase data before recycling IT assets.

## 2. LITERATURE REVIEW AND RELATED WORK

Secure data destruction has become an essential component of modern cybersecurity practices. Several studies have explored techniques for ensuring safe disposal of storage devices and preventing unauthorized data recovery.

Research on secure storage sanitization standards highlights the importance of overwriting disk sectors using approved guidelines such as NIST Special Publication 800-88, which recommends multiple overwrite passes to ensure data irrecoverability[2]. These methods significantly reduce the possibility of recovering previously stored information from physical storage media.

Another widely recognized data destruction method is the DoD 5220.22-M standard, developed by the United States Department of Defense[3]. This approach involves overwriting data multiple times with different bit patterns to eliminate residual magnetic traces on storage devices.

Recent advancements in enterprise IT asset management emphasize integrating device lifecycle tracking with secure data destruction systems. Centralized management platforms allow organizations to maintain records of device ownership, operational status, and disposal procedures, improving accountability and transparency.

Cloud-based and microservice-based architectures have also been widely adopted in cybersecurity applications due to their scalability and modular design[7]. Microservices allow complex systems to be divided into smaller independent components that can be developed, deployed, and maintained efficiently. Despite these developments, many existing solutions lack integrated features such as real-time wipe monitoring, multi-tenant enterprise support, and verifiable audit logs. The proposed system addresses these gaps by combining secure wiping algorithms, device management, and real-time monitoring within a scalable microservice architecture.

## 3. SYSTEM ARCHITECTURE

The proposed system follows a distributed architecture consisting of three major components: the Frontend Interface, Backend Microservices, and a Local Device Agent.

Users interact with the system through a web interface developed using Next.js, which provides a responsive and interactive dashboard for device management and wipe monitoring. The frontend communicates with backend services through secure API calls.

The backend layer is built using Spring Boot microservices, which handle authentication, asset management, wiping control, and logging operations. Each service operates independently, ensuring scalability and modularity.

A Java-based Local Device Agent is installed on user systems to perform hardware-level operations such as detecting connected storage devices and executing disk wiping algorithms. The agent communicates with the backend server through secure API channels.

The system architecture enables seamless communication between hardware and web-based management platforms while maintaining high security and reliability.

## 4. METHODOLOGY

### 4.1 Device Detection and Asset Registration

The Local Device Agent scans the host system for connected storage devices including HDDs, SSDs, and external drives. Device information such as model number, storage capacity, and serial number is collected and transmitted to the backend server for registration in the asset management database.

### 4.2 Secure Data Wiping Process

Once a device is registered, users can initiate the secure wiping process. The system supports multiple wiping algorithms, including:

- NIST 800-88 Standard Wipe
- DoD 5220.22-M Multi-pass Wipe
- Single-pass Overwrite

During the wiping process, disk sectors are overwritten with random or predefined data patterns to eliminate recoverable traces of previously stored information.

### 4.3 Real-Time Monitoring

Real-time monitoring of wipe progress is implemented using WebSocket communication. The backend server continuously sends status updates to the frontend dashboard, allowing users to observe the wiping progress through visual progress indicators.

### 4.4 Multi-Tenant Architecture

The system supports multiple organizations through a multi-tenant architecture. Each tenant maintains independent users, assets, and wiping logs, enabling the platform to operate as enterprise SaaS software.

### 4.5 Audit Logging

All system activities such as login attempts, device imports, wipe operations, and administrative actions are recorded in audit logs. These logs provide verifiable proof of data destruction and support compliance requirements.

## 5. IMPLEMENTATION AND RESULTS

The system was implemented using Java 21, Spring Boot, and Next.js, with MySQL serving as the primary database engine. The platform was deployed using containerized services to ensure scalability and efficient resource management.

Experimental testing was conducted using multiple storage devices to evaluate the functionality of the data wiping algorithms and system monitoring capabilities. The results demonstrate that the system successfully performs secure data wiping operations while providing real-time monitoring through the web interface. Device detection and asset tracking features allow administrators to maintain a centralized inventory of storage devices.

The integration of audit logs ensures transparency and accountability by maintaining records of all wiping operations. Overall, the system effectively meets the requirements of secure IT asset recycling management.

## 6. DISCUSSION

The implementation of the Secure Asset Wiper platform demonstrates the effectiveness of integrating cybersecurity principles with modern web-based technologies. The use of microservice architecture allows the system to scale efficiently as the number of devices and users increases.

Real-time monitoring using WebSocket technology improves user experience by providing instant updates during the wiping process. This feature is particularly useful for enterprise administrators who need to track multiple devices simultaneously.

The use of standardized wiping algorithms such as NIST 800-88 ensures compliance with internationally recognized data destruction guidelines[2]. Additionally, audit logging enhances transparency and provides verifiable proof of secure data deletion.

However, the system currently relies on local device agents for hardware access, which requires installation on each user system. Future developments may focus on improving remote device management capabilities and cloud-based deployment models.

## 7. CONCLUSION

This research presents a secure and scalable platform for managing IT asset recycling and secure data destruction. The proposed Secure Asset Wiper system integrates device detection, secure wiping algorithms, asset tracking, and real-time monitoring into a unified platform.

The system ensures reliable data destruction before device recycling, preventing potential data leakage and improving cybersecurity practices within organizations. The implementation demonstrates that combining microservice architecture, web technologies, and local device agents provides an effective solution for enterprise IT asset management.

Future work will focus on enhancing the platform with advanced features such as automated wipe certification, blockchain-based verification, and cloud deployment capabilities to further improve transparency and scalability.

## References

[1] Gutmann, P. (2001). Secure Deletion of Data from Magnetic and Solid-State Memory. University of Auckland, New Zealand, Technical Report.

[2] National Institute of Standards and Technology (NIST). (2014). Guidelines for Media Sanitization. NIST Special Publication 800-88 Revision 1.

[3] U.S. Department of Defense. (2006). National Industrial Security Program Operating Manual (DoD 5220.22-M). U.S. DoD, Washington, DC.

[4] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.

[5] Bishop, M. (2018). *Computer Security: Art and Science* (2nd ed.). Addison-Wesley.

[6] Tanenbaum, A. S., & Bos, H. (2019). *Modern Operating Systems* (4th ed.). Pearson.

[7] Newman, S. (2021). *Building Microservices: Designing Fine-Grained Systems*. O'Reilly Media.

[8] Fowler, M. (2018). *Patterns of Enterprise Application Architecture*. Addison-Wesley.

[9] Fielding, R. (2000). Architectural Styles and the Design of Network-Based Software Architectures. Doctoral Dissertation, University of California, Irvine.

[10] Gamma, E., Helm, R., Johnson, R., & Vlissides, J. (1994). *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley.

[11] Schneier, B. (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley.

[12] Viega, J., & McGraw, G. (2019). *Building Secure Software: How to Avoid Security Problems the Right Way*. Addison-Wesley.

[13] Smith, S., & Marchesini, J. (2008). *The Craft of System Security*. Addison-Wesley.

[14] OWASP Foundation. (2021). OWASP Top 10 Web Application Security Risks. OWASP Project.

[15] Bernstein, D. (2022). Understanding Data Destruction and Secure Disk Wiping Methods. *Journal of Information Security*, 12(3), 145-152.