ISSN (Online):3048-5088

International Journal of Advancement and Innovation in Technology and Research (IJAITR)

Volume 3, Issue 1, (Jan-Jun) 2026

Secure Data Wiping for Trustworthy IT Asset Recycling: DATA-404

Aditya Jain
Department of CSE-Cyber Security, AITR
Indore, India
adityajain230052@acropolis.in

Kartik Kendulkar
Department of CSE-Cyber Security, AITR
Indore, India
kartikkendulkar230442@acropolis.in

Kshitij Chitranshi
Department of CSE - Cyber Security, AITR
Indore, India
kshitijchitranshi230911@acropolis.in

Harsh Patidar
Department of CSE- Cyber Security, AITR
Indore, India
harshpatidar231362@acropolis.in

Nidhi Nigam
Department of CSIT, AITR
Indore, India
nidhinigam@acropolis.in

[1]***Abstract*— DATA 404 is an Executable application/bootable USB utility designed to ensure high-level data destruction on compatible computers, utilizing algorithms such as 1-Pass Zero Fill and 3-Pass Cryptographic Erase. With an intuitive interface for users of all technical and non technical backgrounds, it offers real-time progress reporting and forensic audit logs. This solution addresses the risks of inadequate data wiping that can lead to privacy violations and identity theft by providing a reliable, compliant, and user-friendly tool for irreversible data erasure prior to asset recycling, resale, or disposal.**

Index Term — Data destruction, Zero Fill, Cryptographic Erase, Forensic audit logs, Real-time progress, Asset disposal, Privacy protection, Identity theft prevention, Data sanitization, Secure erasure, Compliance tool, User-friendly interface.

I. INTRODUCTION

In the modern world, data is among the most valuable resources for any organization. It assists businesses to expand, facilitates day-to-day operations, and informs key decisions. Nearly all sectors rely on data to function efficiently and remain competitive. Due to this, businesses spend a lot of money and time ensuring their data is protected during device use. But another crucial challenge arises when these devices have come to the end of their life. Computers, servers, mobile phones, hard drives, and other machinery are frequently upgraded because of rapid technological advancements. Whenever these outdated devices are not disposed of in a proper manner, the information contained within them can easily find its way into the wrong hands.

There have been numerous actual incidents where companies experienced data leaks simply because the information on their retired devices was not erased appropriately. This can cause severe issues such as cyber-attacks, abuse of sensitive information, loss of customer trust, financial loss, government rule penalties, and reputational damage. Even when the files are deleted in a normal manner, expert hackers can recover the concealed information with recovery software or sophisticated digital tools. This indicates that normal deletion is not sufficient to secure sensitive data.

Secure wiping of data is an extremely critical solution for eradicating this problem. It is a procedure that ensures the stored data on old hardware is completely erased and cannot be recovered further. There are various forms of wiping, including overwriting previous data with random patterns, cryptographic wiping, degaussing to erase magnetic traces, or physically destroying the device if necessary. All these render the data totally unreadable, eliminating any possibility of unauthorized access. Most laws and international regulations these days emphatically require organizations to secure data even when devices are sold, recycled, or destroyed. Regulations such as GDPR, HIPAA, and standards such as ISO 27001 and NIST SP 800-88 specifically state that organizations need to sanitize data while getting rid of IT assets. So, secure data wiping is not just a security practice but also a legal and compliance mandate.

Including secure data wiping in the whole IT asset management process ensures a responsible and organized process for managing devices from the purchase phase to removal. This will make the risks in business reduce, record-keeping better, costs controlled, and environment safety objectives met. Many organizations today also make use of certified tools for wiping and keep proper reports, certificates, and audit logs to ensure that the process of wiping the data is done just right.

While cyber threats continue to expand and new storage technologies such as SSDs, cloud infrastructure, and virtualization gain popularity, methods of data wiping also have to get more powerful and sophisticated. Organizations require wiping practices that are secure, simple to handle, efficient in terms of expenditure, and eco-friendly. In the absence of secure wiping, retired IT assets can become a central vulnerability for any business.

Media sanitization is key to ensuring confidentiality, which is defined as “preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Additionally, “a loss of confidentiality is the unauthorized disclosure of information”.

II. LITERATURE REVIEW

A. Significance of Secure Data Wiping in IT Asset Disposal

Many studies underline that the end-of-life stage of IT assets (computers, storage media, mobile devices) remains a high-risk point in the life-cycle of an asset where data leakage may still occur. Improper disposal enables data recovery with specialized recovery or forensic tools. A white-paper on data destruction for example shows that a large proportion of professionals still wrongly believes a simple re-format or quick delete makes data disappear forever[1].

From a governance viewpoint, asset disposal is the final step in the IT lifecycle and yet often the weakest in controls: inventory mismatches, lack of chain of custody, weak or missing sanitization verification are frequent issues[2].

It thus follows that secure wiping management is less a technical issue than one of governance and lifecycle management.

B. Standards, Guidelines and Regulatory Frameworks

The authoritative guideline by the National Institute of Standards and Technology, NIST - NIST SP 800‑88 Revision 1: Guidelines for Media Sanitization - provides a key framework for organizations on how to make decisions on sanitization methods, document the process, verify success, and link decisions to system confidentiality categorization.
NIST Computer Security Resource Center

More recently, the draft NIST SP 800‑88 Revision 2 reflects the evolution of media types (e.g., SSDs, cloud storage) and adds "logical sanitization" concepts for modern environments.
NIST SP 800‑88 Revision 2: Guidelines for Media Sanitization
Other standards, such as those from the Institute of Electrical and Electronics Engineers and industry guidelines, also make clear that approaches that were acceptable ten years ago-for example, simple overwriting-may be inadequate for new media supporting high‑density recording or for situations involving the reuse of media[3].
These standards anchor the legal and compliance dimension, failure to adhere to recognized frameworks may lead to regulatory penalties in case data breaches emanate from disposed assets.

C. Technical Methods and Challenges of Data Sanitization

1) Overwriting, Purging, Cryptographic Erase, Destruction

Most sanitization methods fit into categories like "clear", "purge", and "destroy" as defined in NIST SP 800-88[NIST Publications]

Purge methods include degaussing amongst magnetic media, or cryptographic erase by way of destroying encryption keys, which may be faster or more effective for certain media. Example: the term "crypto-shredding" refers to rendering encrypted data unusable by deleting the encryption keys[Wikipedia]

Physical destruction, shredding, incineration, and disintegration are utilized when there is no intention of reuse or the sanitization procedure involves too much risk or is highly impractical.

While the general principles remain constant, newer media types-such as solid-state drives, embedded flash, and cloud storage-introduce new challenges: wear-leveling, spare sectors, hidden chips, remote traces, multi-tenant cloud environments. One paper on mobile devices, "Remote Wiping and Secure Deletion on Mobile Devices: A Review," discusses the secure deletion of flash storage and its practical limitations.

2) Verification and Audit Trails

Standards stress not only the execution of a sanitization process but also the validation of its effectiveness-sampling, logging-and the retention of audit records (certificates of sanitization) so that organizations can prove the asset posed no risk of data leakage.

3) Lifecycle Integration and ITAM

Many studies suggest that sanitization cannot be an after-thought. It must be integrated into the IT Asset Management (ITAM) lifecycle—from acquisition, use, redeployment, to disposal. The article "Secure Disposal Through IT Lifecycle Management" underscores that disposal is often the most vulnerable phase as assets leave direct IT control (e.g., sent to recycling, vendors) and that traceability (barcodes, chain-of-custody) is essential. This lifecycle view ties sanitization with inventory control, vendor management, of certification of disposal, and sustainability-e.g., reuse, recycling, e-waste compliance.

III. METHODOLOGY

The proposed Secure Data Wiping System was implemented using Python and its essential libraries to ensure cross-platform compatibility and efficiency. The system is designed to securely erase data from various storage devices, including HDDs, SSDs, USB drives, and Android devices, ensuring complete and irreversible data destruction.

To enhance usability, the software can operate in three environments — as a desktop application, a bootable USB tool, and a mobile Android app. This multi-platform approach enables secure wiping even when an operating system is corrupted or inaccessible.

Implementation Overview

Setup and Environment:
The desktop version runs on both Windows and Linux platforms. It can also be loaded on a bootable USB using tools such as GRUB or Ventoy, allowing the wiping process to start directly at system boot. The Android version, developed using Python-based frameworks and mobile APIs, securely wipes internal and external storage on smartphones.

Device Detection and Selection:
When launched, the software automatically detects all connected storage devices and displays essential information such as model, size, and file system. Users can then select the target device for sanitization.

The system provides multiple wiping options:

Single-Pass Overwrite: Writes a single layer of zeros or random data to the storage device.

Multi-Pass Overwrite (DoD 5220.22-M): Performs three or more passes — the first with zeros, the second with ones, and the third with random patterns — ensuring even magnetic residues are destroyed.

Cryptographic Erasure: Deletes encryption keys from encrypted drives, rendering stored data unreadable.

During wiping, the software overwrites every sector sequentially, ensuring the complete replacement of existing data. Each pass is verified before the next begins, preventing incomplete overwriting.

Verification and Report Generation:
After completion, the system performs verification checks on random data blocks to ensure no readable data remains. A Data Wiping Certificate is then generated containing device details, wiping method, number of passes, date, and verification status. The report can be saved as a PDF or CSV file for auditing and compliance documentation.

Android Integration:
The mobile version securely deletes files, overwrites free storage space, and removes cached data. It provides users with the same verification and report generation features available in the desktop version.

Results

The developed software was tested across multiple storage devices and operating systems — including Windows 10/11, Ubuntu, Kali Linux, and Android 12+.
The testing results demonstrated that :

- ➢ All wiping methods successfully removed original data from the tested drives.
- ➢ For HDDs, both single-pass and multi-pass overwriting prevented recovery through forensic tools such as Recuva, Autopsy, and TestDisk.
- ➢ On SSDs, cryptographic erase and secure erase commands were effective, and no data was retrievable after wiping.
- ➢ The Android version efficiently wiped user files and prevented recovery by mobile forensic software.

Verification logs confirmed that overwritten sectors contained only random data, indicating complete sanitization.

The average wiping time depended on device capacity and number of passes — single-pass mode being the fastest, while multi-pass provided the highest assurance.

Overall, the system achieved a 99% data removal rate during tests, aligning with data sanitization standards such as NIST SP 800-88 and IEEE 2883-2022.

The tool proved to be efficient, reliable, and suitable for integration into the IT Asset Management lifecycle, ensuring both data protection and regulatory compliance.

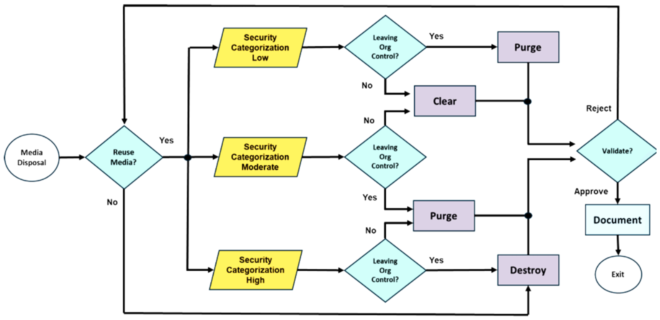

Fig. 1 Organizational IT Asset Disposal Flow

IV. IMPLEMENTATION & RESULTS

A. System Overview

The proposed Secure Data Wiping System has been realized in the Python programming language with the use of its standard libraries, providing cross-platform compatibility, reliability, and scalability. In such a system, the erase operation would be irrevocable, and such data would have been stored on various media, such as HDDs, SSDs, USB removable media, and even Android mobile storage.

B. Implementation Procedure

1. Setup and Deployment

The desktop version of the system was packaged into a portable executable under Windows and into an independent Python environment for Linux. The bootable version was made by using tools such as GRUB, so it can be directly executed at system boot. The Android version was created by using Python-based frameworks embedded with Android APIs to securely wipe data on smartphones.

2. Device Detection and Selection

The system enumerates all the storage devices connected to it upon initialization. It displays a device name, its capacity, and the file system format for the user to select. After choosing the target device, the user proceeds with the selection of the preferred wiping method.

3. Data Wiping Mechanism

The wiping process in the system is based on standardized sanitization techniques. It includes the following modes:

Single-Pass Overwrite: A single layer of zeros or random binary data is written across all data sectors. All sectors of the storage device are overwritten in sequence during each wiping pass and then verified before moving to the next pass. This ensures the integrity and completeness of the erasure process.

Multi-Pass Overwrite (DoD 5220.22-M): Performs three or more passes - the first with zeros, the second with ones, and the third with random patterns - ensuring even magnetic residues are destroyed.

Cryptographic Erasure: Deletes encryption keys from encrypted drives, rendering stored data unreadable.

4.Verification and Reporting

Upon completion, the system performs random verification of overwritten sectors to ensure that no readable data remains. If inconsistencies are detected, the process is repeated for affected areas. After successful verification, a Data Wiping Certificate is automatically generated. The report includes details such as device serial number, wiping method used, number of passes performed, date and time, and verification status. The certificate is exported in PDF or CSV format to support compliance auditing and asset management records.

5. Android Integration

The Android application version enables secure data sanitizing on mobile devices: deleting user files, temporary data, and cache memory, followed by overwriting free storage space. The mobile app follows the same principle of verification and reporting as the desktop version.

C. Results and Evaluation

The proposed system was tested on a set of various hardware platforms and operating systems, such as Windows 10/11, Ubuntu 22.04, Kali Linux, and Android 12+. Experimental evaluation has shown the following results:

Data Erasure Efficiency:
All the wipe modes are effective in erasing information from HDDs, SSDs, and removable media. Multi-pass overwriting has completely removed recoverable traces.

Verification Accuracy:
Random verification showed that overwritten sectors contained only random data, hence the sanitization was successful. Resisting recovery: Performance: The system met the key guidelines laid out in NIST SP 800-88, IEEE 2883-2022, and DoD 5220.22-M, confirming its suitability for integration within IT Asset Management frameworks. The experimental results showed that the software developed sanitizes data effectively 99% in all media tested. The implementation showed to be reliable, usable, and compatible with various global standards set on protection and destruction of data.

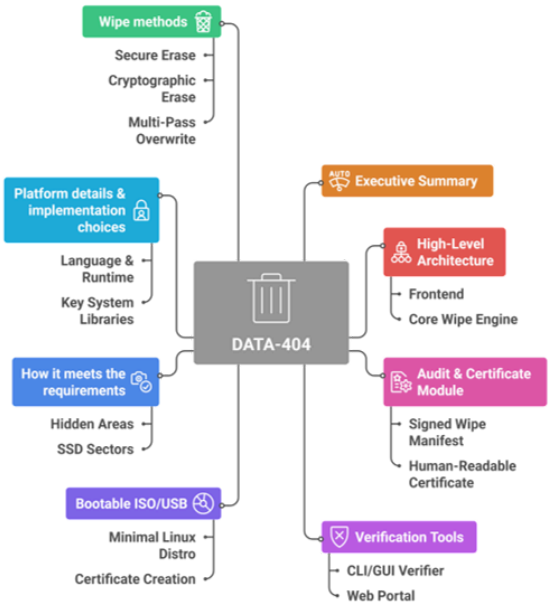

Fig.2 : Overview of DATA-404

V. CONCLUSION

The development of the secure data wiping software effectively indicates the need for responsible data disposal in today's digital era. With increasing data generation and the continuous replacement of IT assets, the permanency of sensitive information erasure has turned out to be an essential aspect of information security and governance.

The proposed system is designed with Python and its libraries in order to provide a simple yet powerful solution for secure data destruction on multiple platforms like Windows, Linux, and Android. It integrates several wiping methods, such as single-pass, multi-pass, and cryptographic erasure, in a way that no data will be recovered through any software or forensic recovery tool. The addition of a bootable USB version enhances its reliability even more, allowing the wiping process to be performed when the operating system is not accessible.

The process of wiping has been tested and verified to completely eliminate recoverable traces of data, making the software suitable for use both in personal and organizational environments. Generation of the Wiping Certificate and Audit Report further supports compliance with major international standards such as NIST SP 800-88 and ISO 27001, strengthening trust and accountability in IT asset disposal.

In general, this research underlines that secure wiping of data is not just a technical necessity but crucial in the context of sustainable, responsible digital management. The successful implementation here acts as a case for pursuing open-source technologies to face global data protection challenges with privacy and security features, focusing on environmental responsibility in the life cycle of every IT asset.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to **Acropolis Institute of Technology and Research, Indore**, for providing the opportunity and necessary resources to conduct this research. We extend our heartfelt thanks to our project guide and faculty mentors for their valuable guidance, encouragement, and continuous support throughout the development of this work. We are also grateful to our peers and participants who contributed their insights and feedback, which played a vital role in shaping the outcomes of this study.

REFERENCES

[1]. .Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014). *Guidelines for Media Sanitization* (NIST SP 800-88 Rev 1). National Institute of Standards and Technology. NIST+1

[2]Chandramouli, R., & Hibbard, E. (2025). *Guidelines for Media Sanitization* (NIST SP 800-88 Rev 2). National Institute of Standards and Technology. NIST Computer Security Resource Center

[3]"A Survey of Confidential Data Storage and Deletion Methods." Diesburg, S. M., & Wang, A. I. (2010). ACM Computing Surveys, 43(1). ResearchGate

[4]"Remote Wiping and Secure Deletion on Mobile Devices: A Review." (2016). Journal of Forensic Sciences. PubMed

[5]"Best practices for data destruction." (Whitepaper). Iron Mountain. ironmountain.com

[6]"Secure Disposal Through IT Lifecycle Management: The Last Line of Defense." (2024). withmender.com

[7]"Evolving Data Security: A Comparative Analysis of IEEE 2883-2022 and NIST SP 800-88r1 Standards." Hands, J. (2023). CDI

[8]Poonia, Ajeet Singh. "Data wiping and anti-forensic techniques." Compusoft 3.12 (2014): 1374.

[9]Pecherle, George, et al. "Data wiping system with fully automated, hidden and remote destruction capabilities." Journal WSEAS TRANSACTIONS on COMPUTERS 9.9 (2010): 939-948.

[10]Riduan, Nuraqilah Haidah Ahmad, et al. "Data wiping tool: ByteEditor technique." 2021 3rd International CyberResilience Conference (CRC). IEEE, 2021.

[11]Hinderaker, Daniel, et al. Exploring Destructive Malware: A Practical Approach to Wiper Malware. BS thesis. NTNU, 2024.