Self-Service Printing Automation: A Retrofit Print Payment Device

Abhang Prajwal[1], Gund Vinayak[2], Sonawane Shubham[3], Prof. Navale N.D[4]
[1,2,3,4]*Samarth College of Engineering and Management,Belhe*

***Abstract*—Traditional public printing services are manual, slow, and pose significant data privacy risks. This paper proposes a "Retrofit Print Payment Device," a compact, IoT-enabled hardware module that converts any conventional printer into a secure, self-service kiosk. The system integrates multi-mode file submission (USB, Wi-Fi) with a secure payment gateway supporting modern methods like UPI and NFC. Its "pay-to-release" workflow, combined with automatic, secure file deletion post-printing, addresses the key gaps in efficiency and data privacy. This device presents a cost-effective, universally compatible solution for automating and modernizing existing print infrastructure.**

***Index Terms*—Self-Service Printing, Retrofit, Print Kiosk, UPI, Secure Payment, IoT, Secure Deletion**

I. INTRODUCTION

Printing remains an essential requirement for students, professionals, and businesses in day-to-day operations. However, traditional printing services, particularly in public spaces, involve multiple manual steps that result in delays and significant security concerns. In the current scenario, customers are required to send their files to a shopkeeper via USB drives, email, or instant messaging applications like WhatsApp. The shopkeeper then manually configures print settings, collects payment separately, and initiates the print job.

This process is beset with several critical issues:

Delays in Service: The workflow is entirely dependent on human operators, creating bottlenecks and long waiting times for users.

Data Privacy Risks: Sensitive documents (e.g., contracts, ID proofs, academic papers) may remain stored on shop computers long after printing, posing a significant privacy breach.

Lack of Integration: There is no automation linking payment confirmation to the actual print release, leading to potential revenue loss for owners and an inefficient user experience. The absence of an integrated, automated system creates inefficiencies and user dissatisfaction. This project addresses these challenges by designing and developing a Retrofit Print Payment Device. This device is a universal, attachable module that integrates with existing printers to automate document submission, securely process payments, and initiate printing without human assistance, bringing ATM-like efficiency and security to the printing industry

II. LITERATURE SURVEY

To establish the novelty of the proposed system, a thorough analysis of prior art, including existing patents and commercial products, was conducted.

[1] US Patent US20040021897A1: This patent, "System and method for remotely managing operations of a printing apparatus," discloses a plug-in "disabler" unit. This device attaches to a printer's power supply and Page 1 of 3 enforces a pre-paid page count by sensing the electric current. This is fundamentally different from our system, as it merely cuts power and does not handle the digital print job, manage modern payment methods, or ensure data deletion. Our device intercepts and manages the digital print job itself.

[2] US Patent US20150124278A1: Titled "Printing with payment validation," this publication describes a cloud-based print service. A user uploads a document, receives a "release code," and pays via a hosted website before the job is sent to the printer. This is a server-centric approach, not a local, attachable hardware module. Our device differs by providing an on-site module that directly connects to the printer, embeds payment (QR/NFC) into the local workflow, and adds an automatic data wipe feature not addressed by the patent.

[3] PALAS Software (India): This company offers a "Self-Service Print Shop" software bundle that runs on a touchscreen PC and integrates with HP printers. It explicitly supports on-screen UPI/mobile wallet payments. This validates the market need for UPI-enabled printing in India. However, it is a full, PC-based kiosk, not a compact, low-cost, universal hardware module that can be "retrofitted" to any existing printer.

[4] PrintWithMe / WithMe (U.S.): This is a cloud-based service where users email documents to a kiosk's address and pay online to release prints. This represents a different, cloud-dependent workflow and is not a local, attachable hardware solution. Summary of Research Gap: Our literature survey confirms a distinct gap. While full kiosks and cloud services exist, no prior art appears to disclose the specific, novel combination of a compact, universal, and cost-effective hardware retrofit module that integrates modern payment gateways (like UPI) and ensures data privacy through secure, automatic file deletion

III. PROPOSED SYSTEM

The proposed "Retrofit Print Payment Device" is an IoT-enabled, universally compatible printing automation module designed to integrate with any existing printer. The system is designed to automate the entire workflow, allowing users to upload documents, make secure payments, and automatically release prints without manual intervention.

System Workflow:

1 File Submission: The user initiates the process by submitting a document via multiple methods, such as a USB drive or Wi-Fi Direct from a smartphone.

2 Print Configuration: Using an interactive touchscreen interface, the user selects print preferences (e.g., page size, color/B&W, number of copies).

3 Payment Processing: The system automatically calculates the total cost based on the settings. It then displays a dynamic QR code for UPI payment or prompts for NFC/card payment.

4 Automated Print Release: The device's central controller communicates with the payment gateway. Only after receiving a successful payment confirmation is the print job released to the connected printer.

5 Secure Data Deletion: To ensure user confidentiality, the system automatically deletes all user files from its local storage immediately after the print job is successfully completed

3.1 Software Requirements:

- Programming Languages: Python, Embedded C/C++.
- Frameworks & Libraries: Flask (for backend API), Embedded SDKs (STM32 HAL / ESP-IDF), OpenCV (for file handling/preview), Printer Communication Protocols (PCL, ESC/POS).
- Database: SQLite (for temporary local storage of logs).
- Security: AES-256 Encryption, SSL/TLS Protocols.

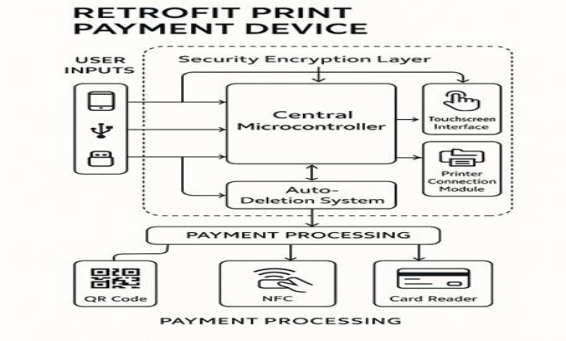
3.2 Hardware Requirements:

- Processing Unit: ARM-based Microcontroller (e.g., STM32) or Single-Board Computer (e.g., Raspberry Pi).
- User Interface: Touchscreen Hardware (Integrated display module).
- Connectivity: USB Host Controllers, Wi-Fi/Bluetooth Modules.
- Payment Hardware: NFC module, QR code scanner, and EMV-certified card reader.

IV. ARCHITECTURE

The proposed system adopts a modular and layered architecture to ensure secure, compatible, and automated print services. This design integrates hardware and software components to deliver a seamless self-service experience while prioritizing data integrity.

4.1 Architecture Diagram



4.2 Module Description

The device is composed of interconnected modules, each performing specific functions:

- User Input Interfaces: Manages file reception from diverse sources like USB drives, mobile devices (via Wi-Fi/Bluetooth), and potentially SD cards. All files enter through the Security Encryption Layer.
- Central Microcontroller: The core processing unit (e.g., Raspberry Pi/STM32) that orchestrates all operations. It calculates costs, manages print queues, and coordinates interactions between all modules, operating securely within the Encryption Layer.
- Touchscreen Interface: Provides the primary user interaction point for selecting print options, confirming details, viewing costs, and displaying payment instructions.
- Printer Connection Module: Translates the print job into a printer-compatible format (PCL, ESC/POS) and releases it to the attached conventional printer only after payment authorization. Ensures broad printer compatibility.
- Auto-Deletion System: A critical component for data privacy. It works with the Microcontroller to securely and permanently erase all user files from temporary storage immediately after printing is complete, adhering to the Encryption Layer's protocols.
- Payment Processing: Handles all financial transactions. It generates dynamic QR codes for UPI, manages NFC tap-to-pay, and integrates with card readers for secure debit/credit payments. It communicates with external Payment Gateway APIs for real-time verification.

4.3 Security & Encryption

The entire core operation, including the Central Microcontroller and Auto-Deletion System, is protected by a Security Encryption Layer. This layer ensures:

- Data Encryption: All temporary files and job data are encrypted (e.g., AES-256) at rest and in transit.
- Secure Transactions: External communication with payment gateways uses SSL/TLS.
- Tamper Resistance: Mechanisms are in place to prevent unauthorized access or data modification.
- Irreversible Deletion: Guarantees that deleted files are truly unrecoverable.

4.4 Development Methodology

The project employs an Agile development methodology to facilitate iterative improvements and rapid adaptation. Key phases include:

1. Requirements & Hardware Selection: Defining functional needs, printer compatibility, payment options, and selecting optimal hardware components (microcontroller, sensors) and communication protocols.
2. Hardware & Firmware Development: Assembling the prototype and developing low-level code for printer communication, file handling, and initial security layer implementation.
3. API Integration: Developing cost calculation logic and integrating Payment Gateway APIs (UPI, NFC) for real-time transaction validation.
4. User Interface Development: Creating the touchscreen GUI for intuitive user interaction, displaying print options, costs, and payment prompts.
5. Testing & Optimization: Comprehensive end-to-end testing, performance optimization for speed and reliability, and security audits of the encryption and auto-deletion mechanisms.

V. EXPECTED OUTCOMES & DISCUSSION

This project is expected to deliver a fully functional, secure, and user-friendly self-service printing solution, significantly upgrading current printing paradigms.

5.1 Key Deliverables

- Retrofit Hardware: A compact, universal device attachable to existing printers (USB/Network).
- Integrated Payment: Support for UPI QR, NFC, and card payments with real-time verification.
- Automated Print Release: Secure print job release only after confirmed payment.
- Intuitive UI: A user-friendly touchscreen interface for all operations.
- Secure File Handling: Encrypted temporary storage and automatic, irreversible deletion of user files post-printing.

5.2 Benefits & Impact

- Cost Efficiency: Enables service providers to upgrade existing printers without costly replacements, making advanced features accessible to small businesses.
- Revenue Assurance: The "pay-to-release" model ensures all print jobs are paid for, minimizing revenue loss.
- Enhanced User Experience: Offers a fast, 24/7, cashless, and self-service printing option, reducing wait times and staff dependency.
- Guaranteed Data Privacy: The core focus on secure file deletion addresses critical user privacy concerns, a major differentiator.
- Modernization: Transforms traditional print services into automated, technologically advanced hubs, meeting modern user demands.

VI. FUTURE SCOPE

Future enhancements aim to further enrich device intelligence, connectivity, and user convenience:

- Remote Cloud Printing: Developing a mobile app/web portal for users to upload documents remotely and retrieve them with a unique code at any device.
- AI-Based Optimization: Integrating AI to analyze print jobs, automatically suggesting optimal settings (e.g., B&W for text-only documents) for cost-saving and efficiency.
- IoT Monitoring: An admin dashboard for remote monitoring of device status, printer health (paper/ink levels), and usage analytics, enabling predictive maintenance.
- Cloud Storage Integration: Direct access to popular cloud platforms (Google Drive, Dropbox) for seamless document selection.
- Blockchain Security: Implementing blockchain for immutable, tamper-proof transaction records.
- Biometric Authentication: Adding fingerprint or facial recognition for enhanced security and convenient access.

VII. CONCLUSION

The "Self-Service Printing Automation" system offers a robust solution to the inefficiencies, high costs, and privacy risks of traditional printing services. By proposing a cost-effective, universal retrofit hardware module, this project provides a novel approach for service providers. Its unique combination of printer compatibility, modern digital payment integration (UPI, NFC, Card), and a "privacy-first" design with secure auto-deletion, fills a clear market gap. This device not only improves operational efficiency and revenue for operators but also delivers a fast, secure, and convenient ATM-like experience for users, pushing public printing into the digital age.

REFERENCES

[1] US20150124278A1, "Printing with payment validation."

[2] PALAS Software, "Self-Service Print Shop Kiosk," palas-india.com.

[3] P. Verma and L. Das, "Design and Development of Self-Service Printing Kiosks with Payment Integration," Journal of Emerging Computing Technologies, vol. 12, no. 3, pp. 155–165, Sept. 2024.

[4] M. Johnson and K. Lee, "Integration of NFC and QR-based Payment Systems in Public Devices," International Journal of Embedded Systems and Applications, vol. 15, no. 4, pp. 211–220, Oct. 2023.

[5] R. Kumar, S. Mehta, and A. Gupta, IoT-based Remote Monitoring and Predictive Maintenance. Singapore: Springer, 2021.

[6] S. Banerjee and T. Wong, "Secure Data Transmission Techniques for Payment Gateways," IEEE Transactions on Information Forensics and Security, vol. 18, no. 2, pp. 345–356, Feb. 2023.

[7] V. Patel, "UPI and Card Reader API Integration for Smart Payment Systems," Proceedings of the 2023 International Conference on Smart Infrastructure and IoT, pp. 78–84, 2023.

[8] T. Nakamura and J. Lee, Cloud Printing Architecture and Security Challenges. Berlin, Germany: Springer, 2022.