Dr. Niveditha, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Hardware Password Manager

Dr. Niveditha HR Assistant Professor, Anushka, Prakruthi, Pratibha S Patil, Thanushree
Dept of ECE, PESCE, Mandya

Abstract- Password security is a major concern in today's digital world. This project presents a Hardware Password Manager using the ESP32 microcontroller. The system generates secure random passwords using the ESP32's Hardware Random Number Generator (HRNG), encrypts them using the XTEA algorithm, and stores them in EEPROM memory. The encrypted passwords are transmitted through UART communication and decrypted on a computer using a Python application. The proposed system provides a secure, reliable, and low-cost solution for password management

Keywords— ESP32, Hardware Password Manager, Hardware Random Number Generator (HRNG), XTEA Encryption, EEPROM, AT24C256, UART Communication, Password Security, Embedded Systems, Cybersecurity

I. INTRODUCTION

Password security is a major challenge in cybersecurity. Software password managers can be vulnerable to malware, phishing, and data breaches. To address these issues, this project develops a standalone Hardware Password Manager using the ESP32 microcontroller.

The ESP32 provides hardware random number generation (HRNG), enabling the creation of highly secure and unpredictable passwords. Generated passwords are encrypted using the XTEA algorithm, stored securely in EEPROM, and transferred to a PC through UART communication.

This system offers a low-cost, reliable, and secure solution for password storage and management in applications requiring strong security.

II. LITERATURE SURVEY

1. Rojas-Muñoz et al. (2022)
The authors proposed a ring-oscillator based True Random Number Generator (TRNG) that produces high-entropy random bits for cryptographic applications. Their work demonstrated that the generated numbers successfully passed standard randomness tests, making them suitable for secure systems.

2. Patel & Gupta (2024)
This study presented a high-speed TRNG based on ring-oscillator jitter effects. The results showed that the design generates reliable random numbers with minimal hardware requirements, making it suitable for embedded security applications.

3. Choi et al. (2021)
The authors analyzed different ring-oscillator TRNG architectures and evaluated their performance using NIST randomness tests. Their findings highlighted important design factors that improve entropy and randomness quality.

4. Keivani & Fathollahi (2015)
This paper introduced a lightweight implementation of the XTEA encryption algorithm for embedded devices. The study showed that XTEA provides strong security while requiring low memory and power consumption.

III. PROBLEM STATEMENT AND OBJECTIVES

Software password managers can be attacked due to predictable randomness and online storage

vulnerabilities. This project solves the problem by designing a hardware-based password manager using ESP32, which generates truly random passwords and stores them securely offline.

- To utilize ESP32's hardware random number generator for password creation.
- To generate and encrypt passwords using the XTEA algorithm.
- To securely store encrypted passwords in external EEPROM (AT24C256).
- To transmit encrypted passwords to a PC via UART communication

IV. DESIGN METHODOLOGY

The Hardware Password Manager is developed using the ESP32 microcontroller as the main controller.

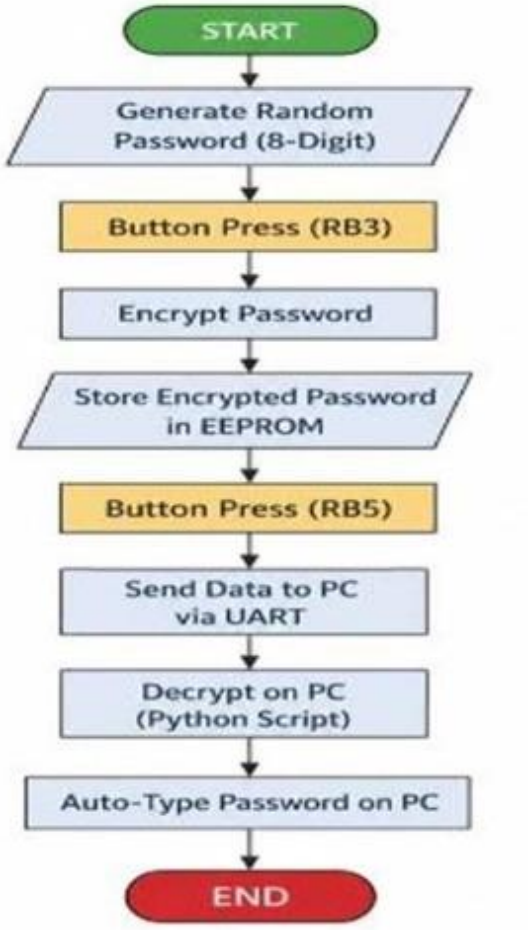

Figure 1: Flowchart of Hardware Password Manager with TRNG

The system generates secure 8-digit passwords using the ESP32's built-in Hardware Random Number Generator (HRNG). The generated passwords are encrypted using the XTEA algorithm and stored securely in an external EEPROM (AT24C256). Users can generate a new password or transmit stored data using push buttons. The encrypted password is sent to a PC through UART communication, where it is decrypted using a Python application to recover the original password.

This methodology ensures secure password generation, storage, and transmission while maintaining low cost and reliability.

Block Diagram

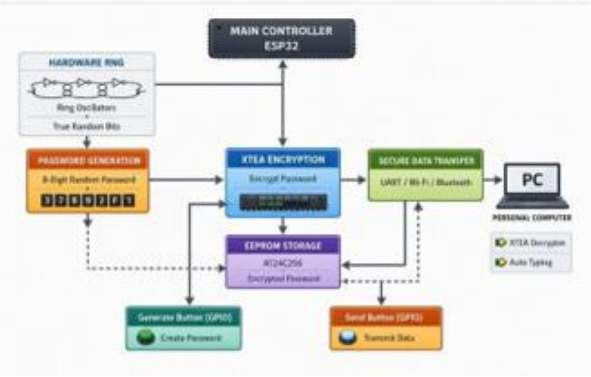

Figure 2: Block Diagram of Hardware Password Manager

V. RESULTS AND ANALYSIS

The proposed Hardware Password Manager was successfully implemented using the ESP32 microcontroller, XTEA encryption algorithm, EEPROM memory, and UART communication. The ESP32's built-in Hardware Random Number Generator (HRNG) generated random 8-digit passwords with high unpredictability. The generated passwords were encrypted using the XTEA algorithm before storage, ensuring data confidentiality.

The encrypted passwords were successfully stored in the AT24C256 EEPROM through I^2C communication and could be retrieved without data loss even after power cycling. Upon pressing the transmit button, the stored encrypted password was sent to a computer through UART communication. The

Python-based receiver application successfully decrypted the received data and recovered the original password.

The system operated reliably during multiple test cycles, demonstrating correct password generation, encryption, storage, retrieval, and transmission.

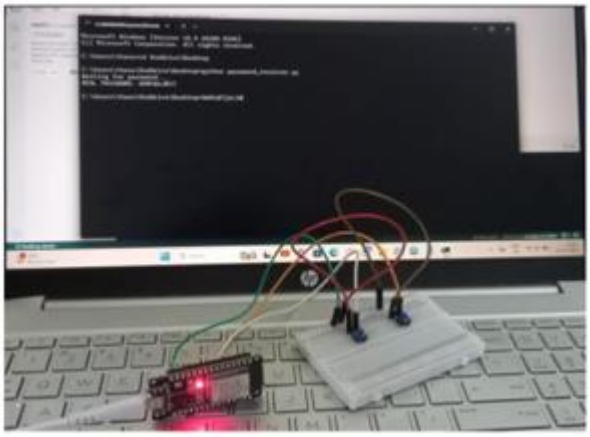

Figure 3: Result of Hardware Password Manager

The developed system provides an effective hardware-based solution for password management. The use of the ESP32's hardware random number generator significantly improves password unpredictability compared to traditional pseudo-random generators. This enhances resistance against brute-force and prediction-based attacks. The XTEA encryption algorithm proved suitable for embedded applications due to its lightweight structure, low memory requirements, and fast execution speed. Encryption ensured that passwords remained protected during storage and transmission. EEPROM storage provided non-volatile memory, allowing encrypted passwords to be retained even when the device was powered off. The storage and retrieval processes were completed accurately without corruption of data. UART communication enabled reliable transfer of encrypted passwords between the hardware device and the computer. Since only encrypted data was transmitted, the risk of password exposure during communication was minimized.

VI. CONCLUSION

Hardware password managers provide a highly secure and reliable solution for protecting sensitive login credentials and personal information. By storing passwords on a dedicated physical device rather than on internet-connected systems, they significantly reduce the risk of hacking, phishing, and malware attacks. These devices offer strong encryption, enhanced privacy, and greater user control over digital security. Although they may involve additional cost and require careful handling, the security benefits they provide outweigh their limitations. As cyber threats continue to increase, hardware password managers remain an effective tool for individuals and organizations seeking stronger password protection and improved cybersecurity.

Acknowledgment

We thank the Department of ECE, PESCE Mandya, for providing the resources and support for successful completion of this project. Special thanks to our mentors and technical staff at the Lab.

REFERENCES

1. "Hardware TRNG on FPGA," River Publishers, 2021.
2. "Analysis of Ring-Oscillator-Based True Random Number Generator on FPGAs," S. Chui, Y. Shin, and
3. H. Yoo, 2021 International Conference on Electronics, Information and Communication (ICEIC), 2021.
4. "Reliable, Secure, and Efficient Hardware Implementation of Password Manager System Using SRAM PUF," M. Mohammadinodoushan, B. Cambou,
5. F. Afgah, C. R. Philabaum, and I. Burke, IEEE Access, Vol. 9, 2021.
6. "Low-Power Ring-Oscillator TRNG for IoT and Smart Cards," Journal of Electrical Engineering, Islamic University of Science and Technology, 2021.
7. "Ring-Oscillator Based True Random Number Generators for Cryptographic Applications,"

International Conference on Electronics and Communication Systems, 2021.
8. "Hardware Security Using Physical Unclonable Functions (PUFs) for Password Management," IEEE Access, 2021.
9. "Design and Analysis of FPGA-Based True Random Number Generators," Electronics and Communication Research Journal, 2021.
10. "Secure Password Storage and Authentication Using Hardware-Based Security Techniques," International Journal of Embedded Systems and Applications, 2021.